JURIDISKA FAKULTETEN

VID LUNDS UNIVERSITET

Emma Bladh

Internet of Things och samtycke enligt dataskyddsförordningen

En undersökning om hur väl dataskyddsförordningens reglering, särskilt gällande samtycke, är anpassad för Internet of Things

JURM02 Examensarbete

Examensarbete på juristprogrammet

30 högskolepoäng

Handledare: Sacharias Votinius

Termin: VT 2023

Innehåll

Summary

The Internet of Things (IoT), i.e. physical objects with embedded electronics that can be connected to the internet and be controlled or exchange data over the network, has become an integral part of many people's daily lives. IoT devices can be anything from fitness trackers and refrigerators to light bulbs and thermostats. However, as is being predicted, we have yet to see the major breakthrough of this technology and what it can be used for. Looking at what IoT devices can do today and what they might do in the future, it is clear that we live in a rapidly changing world where we are on the verge of a new digital era that will revolutionise our lives and everything we do.

However, with the expected explosion of IoT devices in the world, the collection and processing of individuals' personal data will also increase significantly. Since many people have, and will have, IoT devices close to their bodies and in their homes, it means that data is collected from the most personal sphere. This poses major risks to individuals' integrity and right to privacy. It is therefore essential that a legislation is in place that can keep up with technological developments and protect individuals' integrity and human rights. In the European Union, it is primarily the General Data Protection Regulation, more commonly known as GDPR, that is intended to regulate this. The purpose of this paper is thus to investigate how well the GDPR is adapted to this relatively new, but above all rapidly evolving, technology. In order for the study to be carried out within a reasonable framework, it has focused on the legal basis of consent, as this is one of the pillars of the Regulation. The legal basis of consent is also of particular relevance in relation to IoT.

The paper has been written using the legal dogmatic method and the European legal method. The paper has mainly been based on the GDPR, but also guidelines adopted by the European Data Protection Board (EDPB) and the Article 29 Working Party. Other sources used include EU practice, literature and communications and other documents from the European Commission.

The study concludes that the GDPR, with particular regard to the legal basis of consent, is not sufficiently adapted to the IoT to function effectively. Among other things, it fails to regulate the major challenges of IoT technology in relation to individuals' privacy with a reasonable outcome. In this context, it can also be questioned whether consent is at all an appropriate basis for authorising personal data processing in the IoT context. This is because the individual's right to self-determination through consent loses its meaning if the individual, due to the complex technology, cannot have real control over their personal information.

In many cases, there is also no real possibility for IoT companies to de facto comply with the legislation. This is partly because of difficult information problems and partly because it is questionable whether it is even possible for individuals to give a fully genuine and free consent in an IoT context. In addition, the GDPR can often be considered to inhibit technological development. The paper concludes by stating that a separate legislation, that can take specific account of the distinctive and complex nature of IoT and similar technologies, is required in order to better regulate the challenges and conditions of the technology.

Sammanfattning

Internet of Things (IoT), det vill säga fysiska objekt med inbyggd elektronik som kan kopplas upp mot internet och styras eller utbyta data över nätet, har idag blivit en självklar del i många personers vardag. Det kan vara allt från hälsoarmband och kylskåp, till glödlampor och termostater. Som förutspås har vi dock ännu inte sett det stora genombrottet för denna teknik och vad den kan komma att användas till. Vid en inblick i vad IoT-objekt kan göra i dagens läge och vad de kan tänkas utföra i framtiden står det klart att vi lever i en snabbt förändrande värld där vi står på randen till en ny digital era som kommer revolutionera våra liv och allt vi gör.

I och med den förväntade explosionen av IoT-objekt i världen kommer dock även insamlingen och behandlingen av enskildas personliga data att öka markant. Då många har, och kommer att ha, IoT-objekt nära inpå kroppen och i sina hem innebär det att data samlas in från enskildas allra personligaste sfär. Detta innebär stora risker för enskildas integritet och rätt till privatliv. Det är därmed angeläget att det föreligger en lagstiftning som kan hänga med i den tekniska utvecklingen och skydda enskilda personers integritet och mänskliga rättigheter. I Europeiska unionen är det främst dataskyddsförordningen, mer känd som GDPR, som är tänkt att reglera just detta. Syftet med denna uppsats är därmed att undersöka hur väl dataskyddsförordningen är anpassad för denna relativt nya, men framför allt snabbväxande, teknik. För att utföra undersökningen inom en rimlig ram fokuseras den på dataskyddsförordningens lagliga grund samtycke, eftersom denna är en av grundpelarna i förordningen. Den lagliga grunden samtycke är dessutom av särskild relevans i förhållande till IoT.

Uppsatsen har skrivits utifrån den rättsdogmatiska samt den EU-rättsliga metoden. Uppsatsen har i huvudsak baserats på dataskyddsförordningen, men även på riktlinjer antagna av Europeiska dataskyddsstyrelsen (EDPB) och artikel 29-gruppen. Andra källor som använts är bland annat EU-praxis, litteratur samt meddelanden och andra dokument från Europeiska kommissionen.

Slutsatsen av undersökningen är att dataskyddsförordningen, med särskilt beaktande av den lagliga grunden samtycke, inte är tillräckligt anpassad i förhållande till IoT för att funktionera ändamålsenligt. Bland annat lyckas den inte reglera de stora utmaningarna med IoT-tekniken i förhållande till enskildas personliga integritet med ett rimligt utfall. Det kan i detta sammanhang även ifrågasättas om samtycke över huvud taget är en lämplig grund för tillåtelse av personuppgiftsbehandling i IoT-sammanhang. Detta då den enskildes rätt till självbestämmande genom samtycke förlorar sin betydelse om den enskilde, på grund av den komplexa tekniken, inte kan ha en verklig kontroll över sin personliga information.

Många gånger saknas dessutom en reell möjlighet för IoT-företagen att de facto kunna följa lagstiftningen. Dels på grund av en svår informationsproblematik, dels på grund av att det kan ifrågasättas om det ens är möjligt för enskilda att lämna ett helt genuint och frivilligt samtycke i en IoT-kontext. Dessutom får dataskyddsförordningen många gånger anses hämma den tekniska utvecklingen. Uppsatsen avslutas med att konstatera att det som krävs är en särskild lagstiftning som kan ta specifik hänsyn till IoT och liknande teknikers särskiljande och komplexa natur för att bättre kunna reglera teknikens utmaningar och förutsättningar.

Förord

I och med detta examensarbete börjar min tid på juristprogrammet lida mot sitt slut och det är med stolthet jag snart tar min juristexamen. Det har varit några otroligt roliga och givande år som, förutom en gedigen kunskap, gett mig både fina vänner och fina minnen som jag kommer ta med mig genom hela livet.

Jag vill tacka er som hejat på mig, stöttat mig och korrekturläst diverse uppsatser genom hela utbildningen, inklusive detta examensarbete. Utan er hade det inte varit samma sak. Jag vill slutligen rikta ett extra stort tack till Rebecka som har varit en ovärderlig vän och stöttepelare genom hela uppsatsskrivandet.

Emma Bladh

Lund, 23/5 2023

Förkortningar

App	Applikation
Artikel 29-gruppen/WP	Article 29 Data Protection Working Party, omnämns som artikel 29-gruppen i löpande text och WP i noter
Dataskyddsförordningen /förordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
EDPB	Europeiska dataskyddsstyrelsen
EDPS	Europeiska datatillsynsmannen
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
ePrivacy-direktivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
IoT	Internet of Things (sakernas internet)
Kommissionen	Europeiska kommissionen
NFC	Near Field Communication
Prop.	Proposition
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Internet of Things (IoT), på svenska även kallat ”sakernas internet”[1], är ett samlingsnamn för fysiska objekt som kan kopplas upp mot internet och andra nätverk, och därmed styras över internet och inhämta data. IoT-objekt kan dessutom kommunicera och utbyta data med andra enheter och system, genom inbyggda sensorer, mjukvara och andra tekniker. Sådana objekt kan vara allt från hushållsapparater som vitvaror och tv-apparater, termostater, elektroniska larm och lås, till kläder, accessoarer, maskiner, byggnader, bilar, med mera.[2]

Trots att IoT-teknologin har funnits i några decennier är det först nu den börjar ta fart på allvar. Teknikens riktigt stora genombrott på bred front anses av många till och med fortfarande ligga framför oss.[3] Detta beror på att innovationen accelererar och digitala tekniker mognar alltmer, samtidigt som priset för de delar som gör tekniken möjlig sjunker.[4] Transforma Insights räknar exempelvis med att antalet IoT-objekt kommer tredubblas, från 9,7 biljoner år 2020 till mer än 29 biljoner år 2030.[5] Den höga utvecklingstakten visar sig också i att antalet patentansökningar i världen gällande IoT fyrdubblades mellan år 2016 och år 2019.[6] Vid en inblick i vad IoT-objekt kan göra i dagens läge och vad de kan tänkas utföra i framtiden står det klart att vi lever i en snabbt förändrande värld där vi står på randen till en ny digital era som kommer revolutionera våra liv och allt vi gör.

I takt med att tekniken blir alltmer användbar och lättillgänglig tar den också allt större plats i till exempel det offentliga rummet, inom industrin men även i enskildas personliga sfär. Det gör att insamlingen av data från enskilda ökar oerhört, vilket i sin tur resulterar i ett ökat hot mot enskildas integritet och privatliv. Enskildas rätt till skydd och respekt för privatlivet är en mänsklig rättighet som stadgas både i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) samt i Europeiska unionens stadga om de grundläggande rättighet-

[1] Då det mest vanligt förekommande uttrycket för begreppet är Internet of Things, även i Sverige, kommer den engelska termen fortsättningsvis att användas i uppsatsen.

[2] Greengard (2015), s. 15; Integritetsskyddsmyndigheten (2021), s. 68.

[3] Se exempelvis Integritetsskyddsmyndigheten (2021), s. 16 samt Greengard (2015), s. 23.

[4] Greengard (2015), s. 86.

[5] Transforma Insights, “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2023 (in billions)”, *Statista*, hämtad 16 februari 2023, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[6] Integritetsskyddsmyndigheten (2021), s. 60-61.

erna (EU-stadgan).[7] EU-stadgan fastställer även rätten till skydd av personuppgifter som rör den enskilde.[8] Enligt Integritetsskyddsmyndighetens bedömning är IoT ett av de utvecklingsområden som kommer ha störst påverkan på enskildas integritet de kommande åren.[9] Att lagstiftningen hänger med i denna nya teknologiska era är därför av yttersta vikt för att säkerställa ett adekvat skydd för enskildas integritet och mänskliga rättigheter, som annars riskeras att förbises och utnyttjas i företagens jakt på ekonomisk tillväxt.[10]

Allmänna dataskyddsförordningen, EU 2016/679[11], (vidare dataskyddsförordningen/förordningen), mest känd som GDPR, trädde i kraft år 2018 och syftar bland annat till att skydda enskildas grundläggande rättigheter och friheter just när det kommer till datainsamling om enskilda, särskilt personuppgifter.[12] Förordningen är den mest genomgripande reformen av personuppgifter inom EU sedan år 1995 och framställs vara ett steg i EU:s mål att vara världsledande i det datadrivna samhället.[13] Dataskyddsförordningen är det regelverk som är tänkt att skydda enskildas integritet på bred front. Den är nämligen tillämplig när det kommer till allt från marknadsföring och behandling av föreningsmedlemmars uppgifter till registerförda uppgifter på papper och användningen av webbplatser på internet.[14] Frågan måste dock ställas i vilken grad förordningen uppfyller sitt syfte när det kommer till ny och snabbt utvecklande teknik som IoT, som i många aspekter skiljer sig från konventionella tekniker som internet eller vanlig analog databehandling. Är regleringen verkligen anpassad för en ny teknologisk verklighet och kommer den kunna möta dataskyddsrelaterade behov även i framtiden när det kommer till IoT?

1.2 Syfte och frågeställning

Syftet med denna uppsats är att undersöka om dataskyddsförordningen är tillräcklig för att skydda enskildas integritet när det kommer till IoT-objekt. Särskilt fokus läggs på förordningens regelverk om samtycke som laglig grund för behandling av personuppgifter, då detta är en av de mest grund-

[7] Art. 8 i EKMR samt art. 7 i EU-stadgan.

[8] Art. 8 EU-stadgan.

[9] Integritetsskyddsmyndigheten (2021), s. 16.

[10] Att en genomgripande reglering kring dataskydd dock inte ska ses som ett hinder för företags ekonomiska tillväxt, utan tvärtom vara nödvändig för den, framhålls i avsnitt 3.2 nedan.

[11] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning); På engelska: General Data Protection Regulation, förkortat GDPR.

[12] Art. 1.1 och 1.2 dataskyddsförordningen.

[13] Krzysztofek (2021), s. 14; KOM(2020) 264, s. 1; Europeiska kommissionen, ”European data strategy – Making the EU a role model for a society empowered by data”, hämtad 20 april 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

[14] Jfr. art. 2 dataskyddsförordningen.

läggande pelarna i förordningen och som är av särskild relevans i förhållande till IoT. Uppsatsens frågeställning är därmed följande:

- Hur väl anpassad är dataskyddsförordningen, särskilt med beaktande av den lagliga grunden samtycke, i förhållande till IoT?

1.3 Metod och material

För att uppfylla uppsatsens syfte och frågeställning används den rättsdogmatiska och den EU-rättsliga metoden. Den rättsdogmatiska metoden innebär att gällande rätt tolkas och fastställs utifrån de allmänt vedertagna rättskällorna. Rättskälleläran systematiserar det juridiska regelverket och anger en hierarki för hur källorna ska, bör och får tillämpas när gällande rätt uttolkas.[15] Rättsdogmatikens uppgift är alltså att beskriva rättsordningens innehåll, där en domares arbetssätt som utgångspunkt används.[16] En forskare har dock en mer kritisk och långsiktig roll än praktikern, vilket medför att forskaren kan förhålla sig annorlunda till både den juridiska metoden och rättskällorna. Eftersom forskarens uppgift är att granska och analysera har denne möjlighet att ta hänsyn till andra källor än de i rättskälleläran samt förhålla sig annorlunda till källornas innehåll.[17]

Den EU-rättsliga metoden är en del av den rättsdogmatiska metoden och kan betraktas som ett tillvägagångssätt att hantera och tolka just EU-rättsliga källor.[18] Europeiska unionens domstol (EU-domstolen) fastslog i rättsfallet *van Gend en Loos* att EU-rätten utgör en ny rättsordning inom folkrätten.[19] Vid granskning av EU-rätten är därför den EU-rättsliga metoden lämplig eftersom den omfattar singulariteten av EU:s rättssystem, som till skillnad från de flesta nationella rättssystem är ny och saknar samma doktrinära utveckling.[20]

EU-rätten består av primärrätten och sekundärrätten. Primärrätten utgörs av fördragen, EU-stadgan och allmänna rättsprinciper. Den bindande sekundärrätten består av rättsakter som fattats med stöd av fördragen, såsom förordningar, direktiv och beslut. Sekundärrätten består dock även av icke-bindande rättsakter (soft law), såsom yttranden, rekommendationer, resolutioner och meddelanden.[21] Sådana icke-bindande rättsakter har traditionellt sett inte haft en särskilt stark ställning som tolkningsunderlag inom EU. Det har dock på senare tid förekommit att EU-domstolen hänvisar till dessa vid sin tolkning av en rättsakt. EU-domstolen har dessutom konstaterat att när nationell rätt, som antagits utifrån EU-rätten, ska tolkas kan nationella myn-

[15] Kleineman (2018), s. 21.
[16] Olsen (2004), s. 111.
[17] Svensson (2014), s. 222 f.
[18] Reichel (2018), s. 109.
[19] Jfr. mål C-26/62 *Van Gend en Loos*, EU:C:1963:1.
[20] Reichel (2018), s. 110.
[21] Hettne och Eriksson (2011), s. 40-42.

digheter och domstolar ha en skyldighet att använda icke-bindande rättsakter som tolkningsunderlag. Icke-bindande rättsakter har alltså i praktiken inte sällan en stor påverkan på hur EU-rätten ska tolkas.[22]

Eftersom dataskyddsförordningen är föremål för granskning i denna uppsats är det naturligt att förordningen utgör en grundläggande källa. Då EU-praxis har stor betydelse för tolkningen av EU-rätten stöds framställningen även på EU-domstolens domar i viss mån. Den huvudsakliga källan vid tolkningen av dataskyddsförordningens samtycke som laglig grund utgörs dock av riktlinjer antagna av Europeiska dataskyddsstyrelsen (EDPB) under år 2020.

EDPB är ett oberoende EU-organ med syfte att verka för en enhetlig tillämpning av dataskyddsförordningens bestämmelser genom bland annat utfärdande av allmän vägledning. EDPB består av Europeiska datatillsynsmannen (EDPS) samt chefen för varje medlemsstats respektive tillsynsmyndighet.[23] EDPB är inrättad genom artikel 68 i dataskyddsförordningen. I artikeln framgår att EDPB har ställning som juridisk person, vilket stärker organets status i förhållande till dess föregångare, artikel 29-gruppen.[24] Vidare har EDPB befogenhet att fatta bindande beslut gentemot nationella tillsynsmyndigheter.[25] I och med EDPB:s starkare ställning och mer omfattande uppdrag jämfört med artikel 29-gruppen menar Sören Öman[26] att EDPB:s riktlinjer möjligtvis kommer få större formellt genomslag i EU-domstolen än vad artikel 29-gruppens riktlinjer fått.[27] Trots att EDPB framför allt utfärdar allmän vägledning gällande tolkningen av dataskyddsförordningen, det vill säga icke-bindande rättsakter, har dessa alltså ändå stor betydelse för tolkningen och implementeringen av dataskyddsförordningen.[28]

EDPB:s riktlinjer[29] gällande giltigt samtycke enligt dataskyddsförordningen innehåller en omfattande beskrivning av begreppet och utgör därför grunden till kommande granskning av respektive kriterier. EDPB:s riktlinjer om giltigt samtycke är en förlängning och utvidgning av riktlinjerna om samtycke antagna av artikel 29-gruppen.[30] Artikel 29-gruppen motsvarade i princip EDPB:s nuvarande roll, dock i förhållande till det tidigare gällande data-

[22] Reichel (2018), s. 128; jfr. mål C-322/88 *Grimaldi*, EU:C:1989:646.

[23] Art. 68 dataskyddsförordningen; EDPB, ”Om oss”, hämtad 24 april 2023, https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_sv.

[24] Art. 68.1 dataskyddsförordningen.

[25] Art. 65 dataskyddsförordningen; EDPB, ”Om oss”.

[26] Sören Öman är bland annat ordförande i Arbetsdomstolen och har gedigen erfarenhet av arbete i Regeringskansliet och av utredningar inom olika juridiska områden, såsom personuppgiftsskydd.

[27] Öman (2021), s. 28.

[28] EDPB, ”Om oss”.

[29] EDPB, ”Guidelines 05/2020 on consent under Regulation 2016/679”.

[30] Jfr. WP 259, ”Guidelines on consent under Regulation 2016/679”.

skyddsdirektivet, 95/46/EG[31], och inrättades genom artikel 29 i dataskyddsdirektivet.[32] Artikel 29-gruppen utfärdade i slutskedet dock även viss vägledning i förhållande till dataskyddsförordningen.[33] Dessa riktlinjer antagna av artikel 29-gruppen, samt flertalet andra, bekräftades av EDPB i Endorsement 1/2018.[34] Förutom de officiellt bekräftade dokumenten hänvisar EDPB ofta till artikel 29-gruppens yttrande om definitionen av samtycke. Även i den juridiska doktrinen och svenska nationella förarbeten är det vanligt att hänvisa till artikel 29-gruppens riktlinjer. Artikel 29-gruppens dokument kommer därmed också att läggas till grund vid beskrivningen av samtycke enligt dataskyddsförordningen.

Avslutningsvis baseras uppsatsen även på litteratur, artiklar, Europeiska kommissionens (kommissionen) meddelanden och andra källor. Dessa bidrar till en förståelse för det tekniska området IoT samt till att beskriva rättsläget gällande samtycke enligt dataskyddsförordningen.

1.4 Forskningsläge

Vid tiden för publicering av denna uppsats (juni år 2023) har dataskyddsförordningen varit i kraft i fem år. Under dessa år har det publicerats en relativt omfattande del litteratur och artiklar om dataskyddsförordningen. Dessa publiceringar är dock främst av en mer generell karaktär där dataskyddsförordningen beskrivs i sin helhet, utan några särskilt uttömmande beskrivningar eller analyser av mer specifika regleringar. Majoriteten av den litteratur som dock finns angående just samtycke i dataskyddssammanhang gäller regleringar som föregår dataskyddsförordningen, såsom dataskyddsdirektivet. Följaktligen finns det även en begränsad mängd forskning om hur väl samtycke enligt dataskyddsförordningen är lämpad i förhållande till IoT. Det som finns publicerat handlar främst generellt om olika problem som uppstår med IoT-tekniken i relation till dataskyddsförordningen. Någon djupare analys om IoT relaterat till samtycke som laglig grund görs dock inte.

Artikel 29-gruppen har visat sin medvetenhet om integritetsskyddsproblem som kan uppstå i relation till IoT genom sin åsikt WP 223[35]. I denna utger artikel 29-gruppen en relativt omfattande beskrivning av hur det tidigare gällande dataskyddsdirektivet bör tillämpas i förhållande till IoT, som nu får anses ha relevans för samma tillämpning av dataskyddsförordningen. Denna åsikt verkar dock inte tillräckligt kritisk och analyserande i relation till re-

[31] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

[32] EDPB, ”First Plenary of the European Data Protection Board”, hämtad 24 april 2023, https://edpb.europa.eu/news/news/2018/first-plenary-european-data-protection-board_en; art. 29 dataskyddsdirektivet.

[33] Jfr. exempelvis WP 259 samt WP 251, ”Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”.

[34] EDPB, ”Endorsement 1/2018”.

[35] WP 223, ”Opinion 8/2014 on the Recent Developments on the Internet of Things”.

gleringens lämplighet i förhållande till IoT. I stället försöker den alltså endast ge understöd för hur den dåvarande regleringen bör tillämpas. Detta kommer utan tvekan utifrån arbetsgruppens roll som just vägledande och inte utifrån ett utanförstående objektivt perspektiv där den kan inta en kritiserande ståndpunkt angående regleringens lämplighet.

Sammanfattningsvis skrivs denna uppsats i ett läge där det råder brist på forskning fokuserad just på dataskyddsförordningens reglering om samtycke i relation till IoT. Genom att systematiskt utvärdera förordningens kriterier för ett giltigt samtycke och sätta dessa i relation till IoT bidrar denna uppsats till förståelsen av hur väl dataskyddsförordningen egentligen är lämpad för denna alltmer utvecklade teknik.

1.5 Avgränsningar

Denna uppsats ämnar undersöka hur väl dataskyddsförordningen lämpar sig för IoT med fokus på konsumenters användning av IoT-tekniken. Denna sektion av IoT-objekt kallas på engelska ”consumer IoT”. Uppsatsen kommer därför att fokusera på IoT-objekt som används av enskilda i privat sammanhang. Då det till största del är privata aktörer som tillhandahåller produkter och tjänster inom IoT kommer uppsatsen vidare att fokusera på när IoT-objekt tillhandahålls av just privata aktörer. Hur regleringen förhåller sig till myndigheter och andra inom offentlig verksamhet kommer därav inte att behandlas i någon större utsträckning. Analyser och slutsatser som uppkommer i denna uppsats skulle dock i många fall kunna vara tillämpliga även på IoT-objekt och sammanhang utanför denna ram.

Vidare fokuserar uppsatsen mer specifikt på att undersöka hur just kravet på samtycke enligt dataskyddsförordningen lämpar sig för IoT. Det är främst den lagliga grunden samtycke som kommer undersökas. Uppsatsen ämnar inte undersöka alla dataskyddsförordningens regleringar relaterat till samtycke, exempelvis samtycke gällande dataportabilitet eller överföring till tredje land. Ett undantag är samtycke till behandling av känsliga uppgifter[36] samt automatiserat individuellt beslutsfattande[37] som dock diskuteras närmre, eftersom dessa har särskild betydelse i förhållande till IoT.

Enligt dataskyddsförordningen är ett av kriterierna för att ett samtycke ska anses giltigt att det ska vara ett informerat samtycke. Förordningen innehåller flera generella krav på att den enskilde ska erhålla information vid behandling av personuppgifter. Enligt EDPB krävs det inte att alla dessa generella krav på information ska vara uppfyllda för att just ett samtycke ska anses vara informerat och därmed giltigt.[38] Med hänvisning till EDPB:s betydelse för tolkningen av dataskyddsförordningen, som framgår i avsnitt 1.3

[36] Jfr. art. 9 dataskyddsförordningen.
[37] Jfr. art. 22 dataskyddsförordningen.
[38] För vidare diskussion se avsnitt 4.2.4.1.

om metod och material, väljer jag att utgå från EDPB:s uttalande. Uppsatsen kommer därför inte fokusera på alla krav på information som uppställs enligt dataskyddsförordningen, utan enbart på sådan information som krävs för att ett samtycke ska anses vara informerat. Dataskyddsförordningen innehåller vidare flertalet regleringar som har stor relevans gällande IoT, såsom gällande säkerhetsrisker och särskilda rättigheter som tillkommer den enskilde. Då dessa faller utanför ramen för uppsatsen kommer de dock inte att behandlas.

Barn är i många fall exponerade för IoT-objekt då sådana föremål finns i hemmet. Det finns dessutom IoT-objekt som är specifikt riktade mot barn. Dataskyddsförordningen innehåller regler som är avsedda att ge ett synnerligen starkt skydd för barn, särskilt gällande samtycke. På grund av uppsatsens omfång och tidsram för skrivandet kommer denna reglering dock inte att beröras. Av samma skäl kommer inte heller någon analys göras gällande då användaren av ett IoT-objekt har nedsatt förståelseförmåga.

Uppsatsen fokuserar enbart på samtycke i förhållande till användaren av IoT-objektet. Således exkluderas integritetsfrågor och datainsamling kopplat till tredje man. Exempelvis uppkommer intressanta och komplexa frågor hur dataskyddsförordningens krav på samtycke förhåller sig till en gäst som befinner sig i ett hem med datainsamlande IoT-objekt. Detsamma gäller när en person möter en annan person i det offentliga rummet som bär smarta glasögon som samlar in visuell data. Då en sådan undersökning bör resultera i ett stort omfång i sig själv lämnas dessa frågor för framtida arbeten. Vidare undersöks inte heller IoT-objekt som får sägas vara av avgörande betydelse för enskildas liv och hälsa då dessa väcker ytterligare frågor, vilket skulle resultera i en alltför omfattande uppsats. Exempel på sådana IoT-objekt skulle kunna vara inopererade pacemakers eller apparater med syfte att upptäcka kommande hjärtattack eller stroke. Uppsatsen avser dock omfatta hälsorelaterade IoT-objekt som är av en mer frivillig och intressegrundad karaktär, såsom hälsoarmband.

Vidare fokuserar uppsatsen enbart på hur dataskyddsregleringen verkar på EU-nivå. Uppsatsen undersöker inte om eller på vilket sätt svensk eller annan nationell rätt valt att reglera mer specificerande bestämmelser där dataskyddsförordningen ger möjlighet till det. Däremot används i vissa fall utvalda avgöranden och uttalanden från svenska myndigheter, såsom Integritetsskyddsmyndigheten och Högsta domstolen, för att visa på hur dataskyddsförordningen har tolkats. För att förklara vikten av att lagstiftningen värnar om enskildas integritet nämns vidare EU-stadgans samt EKMR:s reglering angående de mänskliga rättigheterna om rätt till skydd för privatlivet samt skydd av personuppgifter som rör den enskilde. Någon grundligare utredning kring innebörden av rättigheterna görs dock inte.

Frågan om hur väl dataskyddsförordningen lämpar sig för IoT har också viss koppling till det nu gällande direktivet om integritet och elektronisk kommunikation, 2002/58/EG[39], (vidare ePrivacy-direktivet), som är lex specialis i förhållande till dataskyddsförordningen. Medan dataskyddsförordningen säkerställer skyddet av personuppgifter så säkerställer ePrivacy-direktivet mer specifikt konfidentialitet vid elektronisk kommunikation. Det vill säga att direktivet fokuserar på integritet vid själva överföringen av kommunikationen. ePrivacy-direktivet kommer dock med allra största sannolikhet att ersättas av en ny förordning, ePrivacy-förordningen, inom en snar framtid. Förslag till den nya ePrivacy-förordningen lades nämligen fram av kommissionen år 2017 och var planerad att träda i kraft år 2018, samtidigt som dataskyddsförordningen. Ikraftträdandet har dock försenats på grund av att medlemsstaterna inte lyckats enas om ett lagförslag. På grund av att ePrivacy-direktivet förväntas bli obsolet inom snar framtid finns det inte mycket skäl till att utföra en djupare analys i förhållande till regelverket. Inte heller skulle en analys av den kommande ePrivacy-förordningen vara särskilt givande eftersom lagtextens innehåll inte står klart då lagstiftningsprocessen kantas av oenigheter. Således kommer både ePrivacy-direktivet och ePrivacy-förordningen att exkluderas i denna uppsats. Det ska dock noteras att en framtida undersökning av ePrivacy-förordningen kan vara givande när denna trätt i kraft.

Denna uppsats utgör en kritisk granskning av rätten de lege lata för att uppfylla framställningens syfte. Någon nämnvärd diskussion utifrån de lege ferenda kommer därmed inte att föras, det vill säga hur rätten bör vara.

Slutligen ska även påpekas att detta är en juridisk uppsats. Den tekniska beskrivningen av IoT kommer därför enbart hållas på en grundläggande nivå för att bidra till läsarens förståelse av området.

1.6 Disposition

Efter det inledande kapitlet följer kapitel två som utgörs av en grundläggande beskrivning av vad IoT är, vilken datainsamling som sker genom tekniken och hur den insamlade informationen kan användas. En grundläggande förståelse för vad IoT innebär och möjligheterna den ger upphov till är väsentligt för att senare kunna utföra en analys av dataskyddsförordningens lämplighet i relation till IoT.

Det följande kapitel tre redogör översiktligt för dataskyddsförordningen, däribland förklaring av centrala begrepp samt de principer som genomsyrar hela regelverket. Redogörelsen är tänkt att ge läsaren en övergripande för-

[39] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).

ståelse för hur lagstiftningen är uppbyggd samt vad som måste beaktas när personuppgifter hanteras.

Kapitel fyra behandlar specifikt dataskyddsförordningens reglering om samtycke som laglig grund. Kapitlet innehåller en djupgående undersökning om vilka kriterier som ställs upp för att ett samtycke ska anses giltigt enligt dataskyddsförordningen. Det innehåller även en undersökning och analys i förhållande till de särskilda reglerna om samtycke relaterat till känsliga uppgifter samt profilering och automatiserat beslutsfattande.

Uppsatsen fortsätter i kapitel fem med en analys och diskussion av den i uppsatsen beskrivna problematiken för att avslutningsvis, i kapitel sex, komma till en slutsats.

2 Internet of Things

2.1 Inledning

För att underlätta för läsarens förståelse av uppsatsens ämne är det nödvändigt att inleda med en grundläggande beskrivning av tekniken IoT. I detta kapitel förklaras därför kort om hur IoT har uppstått, vad IoT är, hur det fungerar, vilka typer av objekt som hör till begreppet samt hur och vad för typ av data som samlas in.

2.2 Bakgrund

IoT utgör den andra vågen av den digitala revolutionen som började med en utbredd användning av datorer under 1970- och 80-talen.[40] Första gången IoT-konceptet med att införa sensorer och intelligens i fysiska objekt anses ha utförts var på 1980-talet på Carnegie Mellon University i USA. Det var några studenter som kopplade upp en Cola-automat mot internet för att kunna se när drycken var påfylld samt om den var kall, för att slippa gå ända till automaten för att kolla det själva. Termen ’Internet of Things’ myntades dock inte förrän år 1999. Det följande årtiondet ökade det publika intresset av IoT-teknologin när allt fler uppkopplade objekt kom ut på marknaden. År 2000 lanserade LG det första smarta kylskåpet, år 2007 lanserades Apples första iPhone som var den första ”smarta” mobilen som var uppkopplad mot internet och år 2009 började Google testa självkörande bilar.[41] Även om det är svårt att peka ut en specifik händelse som särskilt betydelsefull anser många att lanseringen av Apples iPhone var startskottet för IoT-revolutionen då detta var första gången som den stora massan hade IoT-objekt i sina händer.[42] Andra menar däremot att en smartphone inte räknas som ett IoT-objekt.[43] Även om IoT-utvecklingen har varit ett faktum ett tag sägs den dock fortfarande vara i ett tidigt stadium.[44]

2.3 Vad är IoT?

Det finns ingen generellt accepterad definition om vad som är IoT. Det finns dock många försök att rama in teknologin i en definition som är lättbegriplig och tillräckligt omfattande för att visa den stora bredden av vad som inkluderas i termen.[45] Integritetsskyddsmyndigheten beskriver IoT som ett teknikområde med olika apparater, maskiner, mätutrustning och fordon som har inbyggd teknik och internetuppkoppling, men som typiskt sett inte ses som datorer. Dessa enheter ingår i ett nätverk av smarta enheter som kontinuer-

[40] Greengard (2015), s. xiv.

[41] Natalie Marchant, “What is the Internet of Things?”, *World Economic Forum*, hämtad 16 februari 2023, https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/.

[42] Greengard (2015), s. xii-xiii.

[43] Jfr. exempelvis Sundström (2016), s. 21.

[44] Greengard (2015), s. 23; Integritetsskyddsmyndigheten (2021), s. 16.

[45] Hedtjärn Swaling och Johansson (2018), s. 12.

ligt samlar in information, reagerar på den och kommunicerar med andra enheter och med människor.[46] En annan definition är att IoT är ett nätverk av produkter, system och plattformar som är anslutna via enheter som samlar in, lagrar och kommunicerar data med andra enheter, molnprogramvara, infrastruktur samt individer, för att maximera effektiviteten.[47] En del anser att bara genom att prefixet ”smart” läggs till blir en vanlig sak ett IoT-objekt. Exempelvis blir en vanlig termostat en smart termostat, och därmed ett IoT-objekt, när denna programmeras att själv kunna sättas av och på baserat på interaktion med andra apparater.[48] IoT-objekten kan kopplas upp mot internet eller varandra antingen genom sladd eller trådlös teknologi, vilket exempelvis innefattar satelliter, mobilnät, WiFi, Bluetooth och near-field communication (NFC).[49] Många gånger innehåller de sensorer som kan mäta värden i själva objektet eller omgivningen, exempelvis temperatur, elanvändning eller puls.[50]

Exempel på konsumentprodukter som faller in under kategorin IoT är kaffekokaren som du kan sätta i gång på morgonen med hjälp av mobilen medan du fortfarande ligger kvar i sängen. Det finns också hälsoarmbandet som till exempel mäter din fysiska aktivitet, förbränning av kalorier och blodtryck under dagen och kan ge rekommendationer eller varningar utifrån analyser av stora populationer.[51] Fler exempel på IoT-objekt är uppkopplade vitvaror, TV-apparater, lampor, elektroniska lås och larm, kläder och bilar.[52]

Att koppla upp fysiska ting mot internet och bygga in exempelvis sensorer i vardagliga objekt på detta vis utlovar en helt ny sorts bekvämlighet, säkerhet och, genom analyser av den stora mängd data som genereras, potentiella lösningar på några av dagens samhälleliga utmaningar.[53] Det kommer bland annat att effektivisera vår vardag med automatiserade inköpslistor där vi inte själva måste hålla koll på när till exempel riset, tandkrämen eller mjölken börjar ta slut, utan kylskåpet, skafferiet, badrumsskåpet och så vidare kan göra det åt oss. När konsumenten sedan är i mataffären och närmar sig varugången med dessa varor kan konsumenten få en notis om det på sin smartphone. Det hjälper oss också att leva ett mer hälsosamt liv med bättre koll på sömn, vikt och motion samt att få rätt sjukvård i rätt tid.[54] Hälsoövervakningssystem kommer kunna bidra till att möta utmaningarna i ett åldrande samhälle.[55] Tekniken gör det även möjligt för exempelvis rökdetektorer att larma räddningspersonal när en eld uppstår och för termostater att,

[46] Integritetsskyddsmyndigheten (2021), s. 68.
[47] Elvy (2016), s. 840.
[48] Jfr. Hedtjärn Swaling och Johansson (2018), s. 12; Thierer (2015), s. 9.
[49] WP 223, s. 4; Greengard (2015), s. 15 och 49; Integritetsskyddsmyndigheten (2021), s. 68.
[50] Thierer (2015), s. 8; Bugeja, Jacobsson och Davidsson (2016), s. 172.
[51] Greengard (2015), s. 1-4; Peppet (2014), s. 90.
[52] Integritetsskyddsmyndigheten (2021), s. 68.
[53] Brill (2014), s. 205.
[54] Greengard (2015), s. 94.
[55] KOM(2009) 278, s. 2.

förutom att vara mer användarvänliga, optimera elförbrukningen och minska elkonsumtionen och därmed bidra till att konsumenten sparar pengar.[56] IoT-objekt kommer även kunna lära sig våra vanor för att kunna anpassa sig efter våra preferenser och skapa en bättre användarupplevelse.[57] Ju fler sammankopplade enheter det finns, desto större samling av data skapas, vilket i sin tur skapar oändliga möjligheter för vad som kan åstadkommas med tekniken.[58]

Som förstås utgör IoT-objekten en drastisk utveckling från bara internet. Till skillnad från hur kommunikationen ser ut mellan dator och människa, främst med ljus, ljud och beröring (såsom tangentbord, mus eller touch), har kommunikationen mellan IoT-objekt och människa långt fler möjligheter. När det kommer till IoT-objekt kan kommunikationen till och från människan ske genom exempelvis gester, hjärnvågor, närvaro, röst, beröring, kroppsspråk och vibration, för att bara nämna några. Detta sätter långt färre gränser för hur IoT-objekt kan utformas och användas, vilket skapar helt nya förutsättningar för nya innovationer. Det underlättar exempelvis för en simultan användning av IoT-objekt samtidigt som användaren har sitt huvudfokus någon annanstans, som i trafiken eller när personen lagar mat. Detta eftersom personen inte behöver titta på en skärm eller använda beröring, utan kan i stället använda till exempel sin röst eller gester. En del IoT-objekt kan känna av en människas närvaro, var personen är på väg eller tittar samt läsa av kroppsspråk. På så vis kan objekten reagera på och interagera med människan utan att människan själv aktivt behöver ta del av interaktionen – eller ens vara medveten om den.[59] Faktum är att många IoT-objekt är designade för att vara så osynliga som möjligt, för att skapa en smidig och sömlös användarupplevelse.[60]

Som nämndes i bakgrundsavsnittet går utvecklingen av IoT-produkter snabbt framåt och förväntas att växa explosionsartat. Även i de svenska hemmen ökar antalet uppkopplade enheter. I en undersökning utförd av Internetstiftelsen[61] år 2019 framkom att 54 % av den svenska befolkningen över 16 år hade en uppkopplad enhet hemma. Mobiltelefoner och datorer var exkluderade i undersökningen. Det var en ökning jämfört med det föregående året, år 2018, med fyra procentenheter. De flesta uppgav dock att de endast hade någon enstaka uppkopplad enhet hemma, då 39 % av svarspersonerna uppgav att de hade 1-5 uppkopplade enheter hemma. 9 % av svarspersonerna uppgav att de hade 6-10 uppkopplade enheter hemma. Undersökningen visade dock även att många inte vet om man har någon uppkopplad enhet hemma, och sannolikt vad begreppet ”uppkopplad sak” innebär,

[56] Greengard (2015), s. 187.
[57] Sundström (2016), s. 42.
[58] Greengard (2015), s. 86.
[59] Sundström (2016), s. 6.
[60] WP 223, s. 16.
[61] Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation som verkar för ett internet som bidrar positivt till människan och samhället.

då 7 % svarade att de inte visste om de hade någon uppkopplad sak hemma eller inte. Det var samma procent som föregående år.[62] Att det föreligger en okunskap om vad IoT ens är och faktumet att konsumenter kan ha ett eller flera IoT-objekt hemma eller i sin närhet utan att ens veta om det visar särskilt på vikten av att konsumenten görs medveten och informeras om den datainsamling som sker genom objekten.

2.4 Datainsamling som sker genom IoT

Det finns ett stort antal IoT-produkter tillgängliga på marknaden och som framgått tidigare i uppsatsen kommer antalet bara att öka. Det innebär även att mängden datainsamling kommer att öka enormt. Den typ av data som samlas in genom IoT-objekt skiljer sig givetvis åt beroende på vilken typ av objekt det är frågan om, vad den har för funktionellt syfte och därmed vad för teknik som är inbyggd i den. Det kan dock exempelvis nämnas att smarta glödlampor och vattenmätare i duschen kan samla in data om konsumentens el- respektive vattenkonsumtion, såsom vilken tid enheterna används och hur mycket el respektive vatten som förbrukas.[63] Ett hälsoarmband kan mäta antalet gångna steg under dagen, förbrända kalorier och hur många minuters sömn användaren fått.[64] Underhållningssystem som TV-apparater och högtalare samlar in data om funktioner och sökord som används. Hushållsprodukter och köksredskap som dammsugare eller ugnar kan samla in platsdata och driftscheman.[65] Därutöver finns det till exempel smarta röstassistenter, såsom Amazon Echo eller Google Home. Dessa har inbyggda mikrofoner och är programmerade att lyssna efter kommandon som exempelvis ”hey google” för att utföra uppgifter som att dimma belysningen eller spela musik. Eftersom dessa ständigt är aktiverade för att lyssna efter kommandon skulle de till exempel kunna lyssna på privata samtal.[66]

IoT-objekt kan samla in data både explicit och implicit. Med begreppet explicit menas att objektet inhämtar data utan att involvera användaren. Det kan till exempel ske genom sensorer eller tredjepartsapplikationer såsom Facebook. Med implicit menas att data samlas in genom att användaren själv matar in data direkt i systemet. Dessa fall handlar oftast om inledningsfasen då användaren installerar eller registrerar objektet för första gången eller anpassar den för att möta nya behov. Det kan exempelvis handla om att användarna anger namn eller mejladress. Sådan information anges vanligen

[62] Internetstiftelsen, *Svenskarna och internet 2019*, (2019), s. 19, https://svenskarnaochinternet.se/app/uploads/2019/10/svenskarna-och-internet-2019-a4.pdf.
[63] Bugeja (2018), s. 29.
[64] Peppet (2014), s. 2.
[65] Bugeja, (2018), s. 29.
[66] Bugeja, Jacobsson och Davidsson, (2016), s. 173.

genom en mobilapplikation som tillhandahålls av tillverkaren av objektet eller tjänsteleverantören.[67]

Vidare tenderar IoT-objekt att karaktäriseras av datamaximering, det vill säga en överdriven insamling, lagring och delning av personuppgifter, med syfte att lagra sådan data för att den kan vara användbar i framtiden.[68]

Det kan konstateras att integritetsfrågor är ett inneboende problem i IoT-tekniken eftersom insamling av data krävs för att sådana objekt ska kunna tillhandhålla sina tjänster och därmed ha ett värde.[69] Enskilda är dock inte alltid medvetna om vilken personlig data som samlas in om dem eller ifall informationen delas med tredje parter. Enskilda förstår nödvändigtvis inte heller alltid hur lätt det är att extrahera uppgifter om dem och använda dem för andra ändamål än det ursprungliga syftet. Det är alltså inte svårt att se att detta skapar problem för den enskildes integritet och möjligheter att ta vara på sin rätt till privatliv. Dessutom skapar det svårigheter för enskilda att bedöma värdet av sin personliga data.[70]

2.5 Hur kan insamlad data användas?

IoT-tekniken håller på att revolutionera hur vi lever genom att bland annat effektivisera vårt dagliga liv och skräddarsy användarupplevelser utifrån vårt levnadsmönster. Det innebär dock även att objekten genererar information om oss som kan användas för att avläsa hur vi rör oss, vad vi gör, med vem vi interagerar och så vidare. Data om ett hushålls elkonsumtion kan exempelvis visa när någon är hemma, hur ofta hushållet lagar mat, städar eller tittar på TV, åker på semester eller använder träningsutrustning.[71] Vidare kan det dras många slutsatser om en person om man till exempel vet när personen stiger upp på morgonen, om personen sänker innetemperaturen när denne går hemifrån, om personen lyckas hålla liv i sina växter, vad för mat personen äter, om personen brukar träna eller kör vårdslöst i trafiken.[72] Scott R. Peppet[73] menar att detta skulle kunna möjliggöra för exempelvis banker att bedöma om personen är en god kreditrisk, för arbetsgivare att bedöma om de ska anställa personen eller inte, eller för ett försäkringsbolag att bestämma vilken premie som ska betalas.[74]

[67] Bugeja, Jacobsson och Davidsson (2018), s. 145-146; Bugeja, Jacobsson och Davidsson (2016), s. 172.

[68] Wachter (2018), s. 271.

[69] Bugeja, Jacobsson och Davidsson (2018), s. 147.

[70] Bugeja, Jacobsson och Davidsson, (2016), s. 174.

[71] Peppet (2014), s. 110.

[72] Peppet (2014), s. 90.

[73] Scott R. Peppet är professor i juridik vid University of Colorado School of Law, vars verk "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" inte sällan refereras av andra författare i ämnet.

[74] Peppet (2014), s. 89.

Därutöver kan ännu mer information extraheras om en person genom att sammankopplade sensorer, antingen i samma eller i olika IoT-objekt, utbyter information med varandra och skapar en större informationsbild tillsammans. Detta kallas ”sensor fusion” och innebär att flera sensorer tillsammans kan skapa en större informationsbild än vad de hade kunnat göra separat, var för sig. Peppet illustrerar det med att precis som att två ögon kan uppfatta djupseende när de arbetar tillsammans, som inte ett öga var för sig hade kunnat, kan sammankopplade sensorer tillsammans dra oväntade slutsatser.[75] Exempelvis kan ett hälsoarmbands separata mätningar av hjärtfrekvens respektive andning i kombination inte bara visa på användarens träningsrutiner, utan även användarens användning av alkohol och droger.[76] På så vis kan data från en sensor i ett IoT-objekt användas för fler ändamål utöver sensorns ursprungliga syfte, särskilt i kombination med data från andra IoT-objekt.[77]

Med den enorma insamling av data som möjliggörs med hjälp av IoT-objekt skapas vidare ofantliga datasamlingar. Dessa datasamlingar kan genom big data-analyser, det vill säga samkörning och analys av stora mängder data, skapa detaljerade profiler om användaren. Sådana profiler skulle exempelvis kunna berätta om våra preferenser, personligheter, vanor, intentioner med mera.[78] Genom big data-analyser ökar också möjligheterna att identifiera individer utifrån data som ursprungligen inte utgör personlig data. Detta innebär att det blir allt svårare för den enskilde konsumenten att själv kunna bedöma vilken typ av data som är känslig data och i vilka sammanhang.[79]

Vidare uppmärksammar Internetstiftelsen i sin guide om IoT att flera aktörer, både privata och offentliga, kan ha starka intressen av att öka datainsamlingen. Internetstiftelsen menar även att intressen finns av att använda sådan insamlad data för ändamål utöver vad de ursprungligen samlats in för. Exempelvis uppges att det ingår i många IoT-företags intäktsplan att sälja data om användaren till tredje parter. Sådan data skulle, som delvis nämnts ovan, kunna vara av intresse för tredje part exempelvis för jobbrelaterade syften, för försäkringsbolag att bestämma en kunds premie eller i marknadsföringssyften för att kunna rikta rätt reklam till individen.[80] Att personlig data delas med tredje parter är inte alltid något den enskilde ens är medveten om.[81] Även IoT-företagen själva samlar in data om användaren och hur den använder objektet för att ge feedback till produktutvecklarna i syfte att kunna skapa ännu bättre och mer framgångsrika produkter.[82]

[75] Peppet (2014), s. 93.
[76] Natarajan m.fl. (2013), s.123-132.
[77] Peppet (2014), s. 93.
[78] Peppet (2014), s. 90.
[79] Integritetsskyddsmyndigheten (2021), s. 80.
[80] Sundström (2016), s. 42.
[81] WP 223, s. 4.
[82] Sundström (2016), s. 42.

3 Övergripande om dataskyddsförordningen

3.1 Inledning

I följande kapitel redogörs för regler i EU:s dataskyddsförordning som ger en inblick i hur systemet är uppbyggt och som är relevanta i förhållande till syftet med denna uppsats. Dataskyddsförordningen är den lagstiftning som på EU-nivå reglerar behandlingen av personuppgifter. Då det är en förordning innebär det att dataskyddsförordningen är en direkt bindande rättsakt för alla EU:s medlemsstater.

3.2 Bakgrund, syfte och tillämpningsområde

Dataskyddsförordningen trädde i kraft år 2018 och syftar till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras personuppgifter. Förordningen syftar även till att skydda det fria flödet av personuppgifter inom unionen genom en enhetlig reglering.[83] Den nya lagstiftningen motiveras med att det har skett en snabb teknisk utveckling och globalisering med en avsevärd ökning av insamling och delning av personuppgifter. Det uppges i sin tur ha skapat nya utmaningar för personuppgifter och att det därmed krävs en stark och mer sammanhängande reglering kring dataskydd inom EU.[84]

Dataskyddsförordningen är den första genomgripande reformen av EU:s personuppgiftsskyddsregler sedan det tidigare gällande dataskyddsdirektivet som antogs år 1995 och som implementerades i Sverige genom personuppgiftslagen[85]. Den nya förordningen grundar sig på det tidigare direktivet och i skälen till dataskyddsförordningen anges att målen och principerna som var grundläggande i direktivet är fortsatt giltiga i förordningen.[86] Regelverket har dock uppdaterats och moderniserats då internet och nya teknologier fått ökad påverkan på skyddet av personlig data.[87] Dessutom syftar förordningen till att motverka den fragmentering gällande skyddet av personuppgifter som tidigare förelegat då medlemsstater tolkat det föregående direktivet olika.[88]

Att det i dagens samhälle samlas in personuppgifter för flera olika ändamål och på många olika sätt kan resultera i att individen har svårt att förstå hur deras personliga data behandlas.[89] I en undersökning utförd av kommission-

[83] Art. 1.1 och 1.2 dataskyddsförordningen.
[84] Skäl 6 dataskyddsförordningen.
[85] Personuppgiftslag (1998:204).
[86] Skäl 9 dataskyddsförordningen.
[87] Krzysztofek (2021), s. 14.
[88] KOM (2012) 11, s. 2.
[89] EDPB Guidelines 01/2022, s. 8.

en år 2019 visades att EU-medborgare tyckte att skyddet av personlig data är en viktig fråga, men att endast två tredjedelar av de som tillhandahåller personlig data online ansåg sig ha någon form av kontroll över sina personuppgifter. Av dessa var det endast 15 % som ansåg sig ha full kontroll över sina personuppgifter. Vidare var det 30 % som inte ansåg sig ha någon kontroll alls.[90] Kommissionen menar att ett genomgripande skydd av personuppgifter och att konsumenter upplever att de har en tillräcklig nivå av kontroll över sin personliga information är nödvändig för deras förtroende för den digitala marknaden. Bristande förtroende resulterar i att konsumenter tvekar att köpa produkter och tjänster som dessa företag erhåller. Det kan i sin tur hämma utvecklingen av ny teknik, menar kommissionen. En reglering av behandlingen av personuppgifter anser kommissionen därför vara central för den ekonomiska utvecklingen i unionen, en motivering som också syns i skälen till dataskyddsförordningen.[91]

Förordningen är tillämplig på behandling av personuppgifter som helt eller delvis sker på automatisk väg samt på annan behandling än automatisk, om personuppgifterna ingår eller kommer att ingå i ett register. Det finns dock undantag till regeln då förordningen inte ska tillämpas, bland annat om behandling av personuppgifter sker för rent privata syften.[92] Vidare gäller förordningen när den som behandlar personuppgifter, kallad ”personuppgiftsansvarig” eller ”personuppgiftsbiträde”, är etablerad inom EU samt när personuppgifterna som behandlas rör en person, kallad en ”registrerad”, som befinner sig inom EU.[93] Personuppgiftsansvariga och personuppgiftsbiträde kan följaktligen bli föremål för förordningen även om de befinner sig utanför EU under vissa omständigheter[94], vilket visar på den globala betydelsen regelverket har.

För att underlätta förståelsen av regelverket ska i det följande några relevanta centrala begrepp förklaras närmre.

3.3 Centrala begrepp

3.3.1 Personuppgifter

Som nämndes ovan syftar dataskyddsförordningen till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.[95] I förordningen definieras personuppgifter som ”varje upplysning som avser en identifierad eller identifierbar fysisk person […]”, en så kallad ”registrerad”. En identifierbar fysisk person är en person som

[90] Europeiska kommissionen, Special Eurobarometer 487a: The General Data Protection Regulation, (2019), s. 34.
[91] Jfr. KOM(2012) 11, s. 1; KOM(2009) 278, s. 7; skäl 7 dataskyddsförordningen.
[92] Art. 2 dataskyddsförordningen.
[93] Art. 3 dataskyddsförordningen.
[94] Jfr. art. 3.2 dataskyddsförordningen.
[95] Art. 1.2 dataskyddsförordningen.

direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare, såsom namn, identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer, eller en eller flera faktorer som är specifika för den fysiska personens identitet. Dessa kan vara personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.[96]

Med uttrycket ”varje upplysning” signalerar lagstiftaren att begreppet personuppgifter ska tolkas brett. Som förstås genom exemplen ovan kan en personuppgift vara både av objektiv natur, såsom substanser som finns i en persons blod, och av subjektiv natur, såsom en persons åsikter och värderingar. Artikel 29-gruppen beskriver dessutom att en uppgift inte nödvändigtvis behöver vara sann eller bevisad för att informationen ska anses vara en personuppgift. Att förordningen även omfattar uppgifter som är inkorrekta noteras genom reglerna om att en registrerad ska ha rätt att få tillgång till de behandlade uppgifterna om denne samt möjlighet till rättelse och radering.[97]

Begreppet personuppgifter omfattar även känsliga personuppgifter, något som i förordningen benämns som särskilda kategorier av personuppgifter.[98] Känsliga personuppgifter är sådana uppgifter som avslöjar ras[99] eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Det omfattar även genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa, sexualliv eller sexuell läggning. Behandling av känsliga personuppgifter är som huvudregel förbjudet, bortsett från då någon av undantagen är tillämpliga.[100] Det finns anledning att återkomma till detta i avsnitt 4.3 om känsliga uppgifter nedan. Att det som huvudregel är förbjudet att behandla känsliga personuppgifter visar på att dessa har givits ett särskilt skydd.

Vidare omfattar begreppet personuppgifter information som är tillgänglig i vilken form som helst, oavsett om den exempelvis är alfabetisk, numerisk, grafisk, fotografisk eller akustisk. Som beskrevs ovan omfattar personuppgifter även biometrisk data, såsom fingeravtryck, ansiktsstruktur och röster, men kan även inbegripa en djupt rotad färdighet eller andra beteendeegenskaper som exempelvis handskriven signatur, tangenttryckningar, särskilt sätt att gå eller tala och så vidare. Begreppet inrymmer vidare information som lagras till exempel på papper, i ett datorminne med hjälp av binär kod

[96] Art. 4.1 dataskyddsförordningen.

[97] Se art. 15, 16 och 17 dataskyddsförordningen; WP 136, ”Opinion 4/2007 on the concept of personal data”, s. 6.

[98] Se art. 9 dataskyddsförordningen; WP 136, s. 6; Begreppet “känsliga uppgifter” kommer dock att användas i uppsatsen då begreppet är väl inarbetat både på svensk nivå och EU-nivå samt är språkligt enklare att använda och förstå. Dessutom används begreppet i dataskyddsförordningens skäl 10 och 51.

[99] I svensk lagstiftning används inte längre ordet ”ras”. Det används dock i dataskyddsförordningen, men i skälen beskrivs att det inte innebär att EU godtar teorier om att det skulle finnas skilda människoraser, se skäl 51 dataskyddsförordningen.

[100] Art. 9 dataskyddsförordningen.

eller på ett videoband. Ljud- och bilddata inkluderas därmed i begreppet personuppgifter i den mån de presenterar upplysningar som avser en identifierad eller identifierbar fysisk person.[101]

Med en ”identifierad” fysisk person menas en person som i en grupp av människor kan urskiljas från övriga personer i gruppen. Med en ”identifierbar” fysisk person menas en person som det är *möjligt* att identifiera, även om personen inte faktiskt har blivit identifierad ännu.[102] Det krävs således inte att den personuppgiftsansvarige, alltså den som behandlar informationen, själv förfogar över samtliga uppgifter som gör en identifiering möjlig för en uppgift ska räknas som personuppgift.[103]

En person kan bli ”direkt” identifierad genom exempelvis namn. En person kan bli ”indirekt” identifierad genom till exempel ett telefonnummer eller en bils registreringsnummer eller genom en kombination av betydande kriterier som gör det möjligt att identifiera personen genom att skala ner en grupp av människor genom utgallring. Vilken indirekt information som gör det möjligt att faktiskt identifiera en viss person beror på kontexten i den specifika situationen. Exempelvis räcker inte ett väldigt vanligt förekommande namn för att identifiera någon från ett helt lands befolkning. Däremot kan det vara tillräckligt för att identifiera en elev i ett klassrum. Frågan om huruvida informationen kan identifiera en person eller inte, och därmed om det kan räknas som en personuppgift, beror således på omständigheterna i det specifika fallet.[104]

Personuppgifter som har pseudonymiserats[105] omfattas av dataskyddsförordningen, så länge det går att identifiera personen genom kompletterande information. För att avgöra om en person är identifierbar genom den pseudonymiserade informationen bör alla hjälpmedel beaktas, till exempel utgallring, som rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att avgöra om ett hjälpmedel med rimlig sannolikhet kan komma att användas för identifiering av en person bör samtliga objektiva faktorer beaktas, som exempelvis tidsåtgång eller kostnader för identifiering. Även tillgänglig teknik vid tidpunkten för behandlingen såväl som teknisk utveckling bör beaktas. I skälen till dataskyddsförordningen nämns att anonymiserad information inte bör omfattas av förordningen, i den mån den registrerade inte, eller inte längre, är identifierbar.[106] Artikel 29-gruppen menar dock att den stora mängd data som behandlas automatiskt när det kommer till IoT-objekt gör att det skapas en risk för återidentifiering trots att informationen var avsedd att behandlas först efter

[101] WP 136, s. 7-8.
[102] WP 136, s. 12.
[103] Jfr. mål C-582/14 *Breyer*, EU:C:2016:779, punkt 43.
[104] WP 136, s. 12-13.
[105] En pseudonymiserad personuppgift är en personuppgift som behandlats på ett sätt att den inte kan tillskrivas en specifik individ utan kompletterande information.
[106] Skäl 26 dataskyddsförordningen.

anonymisering. Eftersom data insamlad genom IoT därför kan användas för att identifiera en person, trots att viss data anonymiserats, gör att även anonymiserad data kan behöva betraktas som personuppgift.[107]

Som noteras är det ett brett spektrum av information som faller in under dataskyddsförordningens definition av vad som är en personuppgift. Vid en återblick till avsnitt 2.4 om vad för datainsamling det är som sker genom IoT står det vidare klart att en stor del av den data som samlas in genom IoT-objekt direkt eller indirekt kan identifiera en person. Sådan information är därmed att betrakta som personuppgifter och behandling av sådan information faller således in under dataskyddsförordningens regelverk. Så är fallet med exempelvis en uppkopplad ugn som samlar in platsdata eller ett centraliserat belysningssystem som samlar in data om personens elkonsumtion[108]. Detta gäller inte minst då även uppgifter som indirekt kan identifiera en person räknas som personuppgift. Detsamma med att uppgiften endast behöver avse en identifierbar person och att den personuppgiftsansvarige inte själv måste förfoga över samtliga uppgifter som gör en identifiering möjlig.

Det står även klart att en stor del av den data som samlas in är att betrakta som känsliga uppgifter, så kallat särskild kategori av personuppgifter. Det ses inte minst vid hälsoarmband som registrerar uppgifter om den enskildes hälsa, såsom puls eller andning, som tillsammans kan berätta om den enskildes hälsotillstånd, eller röstassistenter som kan registrera biometrisk data som inspelning av röster. En utförligare beskrivning och diskussion kring just känsliga uppgifter förs nedan i avsnitt 4.3.

3.3.2 Behandling och personuppgiftsansvarig

Som nämnts ovan är dataskyddsförordningen tillämplig vid behandling av personuppgifter. Begreppet ”behandling” definieras i förordningen som en åtgärd eller kombination av åtgärder rörande personuppgifter eller uppsättningar av personuppgifter, oavsett om de utförs automatiserat eller inte. I förordningen tas ett antal exempel upp; allt från insamling, ändring och spridning till lagring, radering och förstöring.[109] Även att bara ta del av en personuppgift har ansetts vara behandling av personuppgiften.[110] Begreppet automatisk behandling innefattar all typ av elektronisk behandling.[111]

[107] WP 223, s. 11.

[108] Elkonsumtion kan ses som personuppgift eftersom det är förknippat med en identifierad eller identifierbar person och kan avslöja information om dennes energianvändning och därigenom ge insikt i den registrerades dagliga liv. Se fotnot i EDPS ”Formal comments on the draft Commission Implementing Regulation on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data”, s. 2, samt WP 223, s. 10-11.

[109] Art. 4.2 dataskyddsförordningen.

[110] SOU 2002:18, s. 115.

[111] Frydlinger m.fl (2018), s. 63.

Begreppet behandling är som förstås väldigt brett och omfattar alla former av hantering. Begreppet urskiljer således egentligen inte vilka hanteringsformer som omfattas och inte, eftersom det är svårt att komma på en mänsklig eller automatiserad aktivitet som inte utgör en behandling i förordningens mening.[112] Det är alltså uppenbart att den insamling och hantering av data som sker via IoT-objekt faller in under begreppet behandling och att behandlingen därmed omfattas av dataskyddsförordningen.

Personuppgiftsansvarig är den som, ensamt eller tillsammans med andra, bestämmer ändamålen och medlen för behandlingen av personuppgifter, det vill säga hur och varför personuppgifter behandlas.[113] Detta innefattar såväl tekniska som organisatoriska frågor, såsom vilken plattform som ska användas för behandling, hur länge och var uppgifterna ska lagras samt vem som ska ha tillgång till uppgifterna.[114] Begreppet är ett mycket centralt sådant eftersom det är på den personuppgiftsansvarige som den absoluta majoriteten av alla skyldigheter enligt förordningen åvilar.[115] Till exempel skulle ett IoT-företag som skapar och säljer IoT-objekt alltså vara att betrakta som personuppgiftsansvarig, om det är företaget som bestämmer ändamålen och medlen för personuppgiftsbehandlingen.

Skulle den personuppgiftsansvarige anlita någon annan för att behandla personuppgifter behåller denne sin status som personuppgiftsansvarig och den anlitade får status som personuppgiftsbiträde. Ett personuppgiftsbiträde är nämligen den som behandlar personuppgifter för den personuppgiftsansvariges räkning.[116] Ett exempel på ett personuppgiftsbiträde är när ett företag anlitar en molntjänstleverantör för lagring av personuppgifter. Molntjänstleverantören anses då behandla personuppgifterna för den personuppgiftsansvariges räkning. Den personuppgiftsansvarige behåller alltså då det yttersta ansvaret för att uppgifterna behandlas på ett korrekt och lagenligt sätt.[117]

3.4 Teknologisk neutralitet

Vid reglering av teknik har teknologisk neutralitet länge ansetts vara en vägledande princip.[118] Teknikneutralitet var något som betonades redan i de tidiga stadierna av förberedelserna till dataskyddsförordningen som en viktig del i syfte att skapa en effektiv och modern reglering som skulle kunna möta även framtidens behov av dataskydd.[119] Det har inte funnits någon universellt accepterad definition av begreppet.[120] Enligt kommissionens definition innebär teknikneutralitet dock att regleringen inte bör ”gynna eller

[112] Öman (2021), s. 70-71; SOU 2009:44, s. 92.
[113] Art. 4.7 dataskyddsförordningen.
[114] WP 169, ”Opinion 1/2010 on the concepts of ”controller” and ”processor””, s. 14.
[115] Frydlinger m.fl. (2018), s. 51.
[116] Art. 4.8 dataskyddsförordningen.
[117] Jfr. Öman (2021), s. 89.
[118] Reed (2007), s. 264.
[119] KOM(2012) 11, s. 104.
[120] Reed (2007), s. 266.

missgynna en särskild typ av teknik, utan garantera att samma tjänst regleras på samma sätt, oavsett hur den levereras".[121] Med andra ord ska regleringen alltså ge fullgott skydd till dess skyddsobjekt oavsett vilken teknik som används.

Som tidigare nämnts erkänner dataskyddsförordningen en snabb teknisk utveckling som skapar nya utmaningar för skyddet av personuppgifter och har stor påverkan på ekonomin och det sociala livet. Det framgår även i skälen att tekniken bör underlätta det fria flödet av personuppgifter inom EU samtidigt som en hög skyddsnivå säkerställs för personuppgifter.[122] I skälen till dataskyddsförordningen uppges därför att förordningen bör vara teknikneutral för att skapa en effektiv förordning som är tillämpbar även på framtidens teknik, och för att förhindra att det uppstår en allvarlig risk för att reglerna kringgås.[123] Teknologisk neutralitet uppges alltså vara grundläggande för skyddet av personuppgifter, både med dagens och framtidens teknik, som samtidigt är viktigt för att inte hindra den tekniska utvecklingen. Eftersom tekniken idag utvecklas så snabbt att lagen inte kan hänga med är det dessutom viktigt med en tekniskt neutral reglering för att undvika frekventa revisioner av lagtexten.[124]

3.5 Principer för behandling av personuppgifter

3.5.1 Inledning

För att behandling av personuppgifter ska vara laglig innehåller dataskyddsförordningens artikel 5 ett antal grundläggande principer som genomsyrar hela förordningen. Dessa måste uppfyllas vid varje behandling av personuppgifter. Principerna innebär att en behandling måste omfattas av laglighet, korrekthet (fairness) och öppenhet i förhållande till den registrerade, ändamålsbegränsning, uppgiftsminimering, korrekthet (accuracy), lagringsminimering samt integritet och konfidentialitet.[125] Dessa beskrivs mer ingående i det följande. Som anges i förordningen är det den personuppgiftsansvarige som ansvarar för, och ska kunna visa, att dessa principer uppfylls.[126]

3.5.2 Laglighet, korrekthet och öppenhet

Den första principen som omnämns i förordningen innebär att behandling av personuppgifter måste ske på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.[127] I skälen till förordningen betonas att det bör vara klart och tydligt för registrerade hur, samt i vilken utsträckning, personuppgifter om personen behandlas. Vidare nämns i skälen att öppenhetsprincipen

[121] KOM(1999) 539, s. vi.
[122] Skäl 6 dataskyddsförordningen.
[123] Skäl 15 dataskyddsförordningen.
[124] Reed (2007), s. 268.
[125] Jfr. art. 5 dataskyddsförordningen.
[126] Art. 5.2 dataskyddsförordningen.
[127] Art. 5.1(a) dataskyddsförordningen.

innebär ett krav på att all information och kommunikation, när det rör behandling av personuppgifter, är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används.[128] Artikel 29-gruppen anger uttryckligen att principen om öppenhet gäller under hela behandlingsperioden och inte endast vid den initiala behandlingen.[129] Att behandlingen ska ske på ett lagligt sätt innebär att behandlingen måste ha stöd i lag för att vara tillåten, exempel dataskyddsförordningen men även annan speciallagstiftning.[130]

Vad gäller principen om korrekthet (fairness) har det ifrågasatts i de svenska förarbetena huruvida den svenska termen ”korrekthet” egentligen motsvarar avsikten med bestämmelsen. I andra språkversioner av förordningen, såsom den danska, engelska, franska och tyska, används ord som på svenska snarare skulle översättas till rättvist, skäligt eller rimligt. I den engelska versionen används exempelvis ordet ”fairness”. Dessa andra termer som används i andra språkversioner indikerar, enligt regeringen, att det snarare avses att en intresseavvägning ska göras. Det innebär att även om en laglig grund för behandling av personuppgifter[131] i och för sig skulle vara tillämplig i ett enskilt fall kan det vara oförenligt med principen om korrekthet, och därmed ej tillåtet enligt dataskyddsförordningen, om behandlingen är oskälig i förhållande till den registrerade.[132] I doktrin tas som exempel upp om den personuppgiftsansvarige erhållit personuppgifter genom påtryckningar.[133] Artikel 29-gruppen menar dock att principen om korrekthet (fairness) innebär att den registrerade alltid ska vara fullt medveten om den personliga data som samlas in och behandlas om den.[134] Denna tolkning får anses vara mer i enlighet med skrivelsen i skälen till förordningen, nämligen att det bör klart och tydligt framgå för registrerade hur personuppgifter som rör dem behandlas.[135]

Principen om korrekthet blir enligt artikel 29-gruppens tolkning särskilt relevant i förhållande till IoT. Dels på grund av att objekten ofta samlar in stora mängder data, dels på grund av att de ofta opererar i bakgrunden, med målet att märkas så lite som möjligt av användaren, se avsnitt 2.3 och 2.4. Att IoT-objekt samlar in stora mängder data kan, som tidigare nämnts, försvåra för den enskilde att få inblick i vilken data det är som faktiskt behandlas. Det kan vid sådana tillfällen inte sägas att den registrerade är fullt medveten om den personliga data som behandlas om personen. Det brister därmed i principen om korrekthet (fairness). Samma problematik skapas när

[128] Skäl 39 dataskyddsförordningen.

[129] WP 260, ”Guidelines on transparency under Regulation 2016/679”, s. 6; se även art. 12 dataskyddsförordningen.

[130] Frydlinger m.fl. (2018), s. 35.

[131] Lagliga grunder för behandling av personuppgifter beskrivs närmre nedan i avsnitt 3.6.

[132] Prop. 2017/18:105 s. 47.

[133] Jfr. Frydlinger m.fl. (2018), s. 36.

[134] WP 223, s. 16.

[135] Jfr. skäl 39 dataskyddsförordningen.

IoT-objekt är designade att märkas av användaren så lite som möjligt, vilket kan få användaren att till och med glömma bort att det konstant samlas in data om personen.

Även gällande principen om öppenhet finns problematik i förhållande till IoT. Särskilt när det gäller data som samlas in explicit, det vill säga då IoT-objektet inhämtar data utan att involvera användaren. Det kan ske exempelvis genom sensorer som ständigt samlar in data. I dessa fall kan det vara svårt för IoT-företaget att på förhand veta vilken data som kommer att samlas in, se kapitel 2. Det skapar därmed svårigheter för företaget att på ett lättbegripligt sätt informera användaren om hur och vilken data som kommer behandlas. Dessutom har det i doktrin framförts att det kan vara svårt att på ett lättbegripligt sätt informera om komplicerade dataprocesser som kan ske vid behandling av personuppgifter, såsom sensor fusion och big data-analyser.[136]

3.5.3 Ändamålsbegränsning

Vidare anges att personuppgifter endast ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifterna ska inte heller senare behandlas på ett sätt som är oförenligt med dessa ändamål.[137] Med andra ord är det tillåtet att behandla insamlade uppgifter för andra ändamål än det ursprungligt angivna, dock bara om det nya ändamålet är förenligt med det ursprungliga. Det kan förenklat sägas att den registrerade inte ska bli överraskad över den nya behandlingen.[138] Principen är på så sätt tänkt att å ena sidan möta behovet av förutsägbarhet och rättssäkerhet, å andra sidan behovet av flexibilitet.[139]

I skälen anges att ändamålen för vilka personuppgifterna behandlas för bör vara tydliga och legitima samt att ändamålen ska ha bestämts senast vid den tidpunkt då personuppgifterna samlas in.[140] Genom ändamålsspecifikation sätts således gränser för vilka ändamål den personuppgiftsansvarige kan använda de insamlade personuppgifterna för.[141]

Artikel 29-gruppen tydliggör att ändamålen måste vara tydliga och specifika så att det går att avgöra vilken typ av behandling som ingår och inte ingår i det angivna ändamålet. Ett vagt och allmänt angivet ändamål, såsom ”förbättring av användarupplevelsen”, ”marknadsföringssyften” eller ”för framtida forskning” skulle troligen inte möta kravet på specifikt angivet ändamål utan mer detaljerad information.[142] Om det är svårt att avgöra vilka personuppgifter som behövs för att uppfylla ändamålet är det troligen för vagt och

[136] Wachter (2018), s. 279.
[137] Art. 5.1(b) dataskyddsförordningen.
[138] Frydlinger m.fl. (2018), s. 38; se också art. 6.4 dataskyddsförordningen.
[139] WP 203, ”Opinion 03/2013 on purpose limitation”, s. 5.
[140] Skäl 39 dataskyddsförordningen.
[141] WP 203, s. 15.
[142] WP 203, s. 15-16.

allmänt angivet.[143] Det framhålls dock att hur detaljerat ändamålet ska beskrivas beror på sammanhanget i det enskilda fallet och vilka personuppgifter som är involverade. Att ändamålet ska anges specifikt innebär dock inte att långa och väldigt detaljerade beskrivningar är nödvändiga eller hjälpsamma, utan kan tvärtom få motsatt effekt.[144]

Att de angivna ändamålen ska vara tydliga innebär att det inte ska råda någon tveksamhet kring vad de syftar på eller vara svåra att förstå. Vidare innebär kravet på tydlighet att ändamålsspecifikationen måste förstås på samma sätt, inte bara av den personuppgiftsansvarige och eventuella tredje parter, utan även bland annat av den registrerade.[145]

Slutligen, för att ett angivet ändamål ska vara berättigat måste ändamålet med behandlingen, i likhet med principen om laglighet, vara laglig i bred bemärkelse. Det innebär inte bara att det måste föreligga en laglig grund för behandling enligt förordningen för vilket ändamålet anges. Lagliga grunder för behandling kommer beskrivas närmre nedan. Det innebär också att övrig tillämplig lagstiftning och allmänna principer måste följas, såsom andra dataskyddslagar, arbetsskyddslagar, avtalslagar, konsumentskyddslagar och så vidare. Det innebär även att andra element såsom sedvänjor, etiska regler, avtalsarrangemang och det allmänna sammanhanget ska beaktas vid bedömningen om ett ändamål är berättigat.[146]

Under förutsättning att den data som samlas in endast behandlas för de angivna ändamålen uppstår inte något hinder mot att det ofta är en stor mängd information som samlas in genom IoT-objekt. I likhet med principen om laglighet, korrekthet och öppenhet ovan kan den stora datainsamlingen via IoT-objekt och hur informationen används dock innebära problem i förhållande till principen om ändamålsbegränsning. I och med att tekniken möjliggör att extensiva slutsatser kan dras föreligger en stor risk för att personuppgifter samlas in och behandlas för andra och oförenliga ändamål i förhållande till de ändamål som ursprungligen angavs.

3.5.4 Uppgiftsminimering, korrekthet och lagringsminimering

I dataskyddsförordningen anges vidare att principen om uppgiftsminimering innebär att de personuppgifter som behandlas ska vara adekvata och relevanta.[147] Personuppgifter som är ovidkommande för det angivna ändamålet får därmed inte behandlas.[148] De behandlade personuppgifterna får heller inte vara för omfattande i förhållande till de ändamål för vilka de behand-

[143] Öman (2021), s. 124.
[144] WP 203, s. 16.
[145] WP 203, s. 17.
[146] WP 203, s. 19-20.
[147] Art. 5.1(c) dataskyddsförordningen.
[148] Öman (2021), s. 134.

las.[149] Med andra ord är det inte tillåtet att behandla fler uppgifter än nödvändigt för ändamålet.[150] I skälen anges att principen om uppgiftsminimering även innebär att personuppgifterna endast bör behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel.[151]

När det kommer till IoT-objekt måste personuppgiftsansvariga alltså se till att den information som samlas in är nödvändig för att uppfylla det angivna ändamålet med personuppgiftsbehandlingen. Principen om uppgiftsminimering utmanar således den typiska datamaximeringen när det kommer till IoT-objekt, se avsnitt 2.4, det vill säga tendensen att samla in information för att informationen kan visa sig vara användbar i framtiden.

Principen om korrekthet, eller ”accuracy” som används i den engelska versionen, innebär att de behandlande personuppgifterna ska vara korrekta, och om nödvändigt uppdaterade. Vidare måste alla rimliga åtgärder vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.[152]

Relaterat till IoT-objekt kan det även i förhållande till principen om korrekthet (accuracy) uppstå svårigheter. Personuppgiftsansvariga måste här se till att verifiera användaren av IoT-objektet för att uppfylla principen, speciellt när fler än en person använder objektet. Om användaren inte verifieras skulle personuppgifter från flera olika användare av misstag kunna registreras under en användares profil, vilket skulle leda till att felaktiga uppgifter om den personen behandlas. Det skulle då alltså brista i principen om korrekthet (accuracy).

Principen om lagringsminimering innebär att personuppgifter inte får förvaras under en längre tid än vad som är nödvändigt för ändamålen med behandlingen.[153] Som står i skälen ska perioden för vilka personuppgifterna behandlas vara begränsad till ett strikt minimum.[154] Kopplat till IoT måste det alltså med jämna mellanrum utvärderas om den data som samlats in fortfarande är nödvändig för att uppfylla ändamålen med behandlingen.

3.5.5 Integritet och konfidentialitet

Slutligen ska personuppgifterna behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna. Detta ska göras med användning av lämpliga tekniska eller organisatoriska åtgärder. Att lämplig säkerhet för personuppgifterna ska säkerställas innebär bland annat att personuppgifterna

[149] Art. 5.1(c) dataskyddsförordningen.
[150] Öman (2021), s. 135.
[151] Skäl 39 dataskyddsförordningen.
[152] Art. 5.1(d) dataskyddsförordningen; Öman (2021), s. 140.
[153] Art. 5.1(e) dataskyddsförordningen.
[154] Skäl 39 dataskyddsförordningen.

ska skyddas mot obehörig eller otillåten behandling samt mot förlust, förstöring eller skada genom olyckshändelse.[155]

3.6 Lagliga grunder för behandling

Som tidigare framställts måste den personuppgiftsansvarige, förutom att uppfylla ovan beskrivna grundläggande principer, även ha en tillämplig laglig grund för behandling av personuppgifter för att sådan behandling ska vara tillåten. De lagliga grunder som finns att tillgå hittas i dataskyddsförordningens artikel 6 och är uttömmande. Om ingen av de där uppräknade lagliga grunderna skulle vara tillämpliga är behandling av en persons personuppgifter alltså inte laglig. Artikeln stipulerar att åtminstone en av grunderna ska vara uppfylld. Flera av de lagliga grunderna kan alltså vara tillämpliga och användas på samma behandling samtidigt.[156]

En laglig grund måste vara bestämd för varje specifikt ändamål före behandlingen äger rum och måste kunna påvisas under hela behandlingsprocessen. Detta för att säkerställa ansvarighet och öppenhet enligt de grundläggande principer i dataskyddsförordningen, som redogjordes för ovan.[157]

De lagliga grunderna enligt artikel 6 är följande, citerat:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål
b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås
c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige
d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

[155] Art. 5.1(f) dataskyddsförordningen.
[156] Art. 6 dataskyddsförordningen; prop. 2017/18:105, s. 46; WP 187, ”Opinion 15/2011 on the definition of consent”, s. 8.
[157] Integritetsskyddsmyndigheten, ”Rättslig grund”, *Integritetsskyddsmyndigheten*, senast uppdaterad 17 maj 2022, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/, hämtad 3 april, 2023.

Som Integritetsskyddsmyndigheten skriver är det främst grunderna samtycke, nödvändighet på grund av avtal, nödvändighet på grund av rättslig förpliktelse och nödvändighet på grund av berättigat intresse som är tillämpliga vid privat verksamhet.[158] När det gäller IoT framför artikel 29-gruppen dock att det främst är tre lagliga grunder för behandling som är relevanta. Dessa är samtycke, nödvändighet på grund av avtal samt nödvändighet på grund av berättigat intresse.[159] Då denna uppsats fokuserar på att undersöka hur väl den lagliga grunden samtycke är lämpad för just IoT kommer en fördjupande beskrivning av denna grund att göras i det följande.

[158] Integritetsskyddsmyndigheten, ”Rättslig grund”.
[159] WP 223, s. 15.

4 Samtycke enligt dataskyddsförordningen

4.1 En överblick

Samtycke definieras i dataskyddsförordningen av fyra kumulativa kriterier. Dessa innebär att ett giltigt samtycke måste vara en frivillig, specifik, informerad och otvetydig viljeyttring genom vilken personen godtar behandling av personuppgifter som rör denne. Viljeyttringen kan ske genom ett uttalande eller genom en entydig bekräftande handling.[160] Även om det föreligger ett samtycke som laglig grund för behandling har den personuppgiftsansvarige även en skyldighet att följa de grundläggande principerna i artikel 5, som beskrevs ovan i avsnitt 3.5. Det innebär att även om ett samtycke föreligger skulle behandling av den enskildes personliga uppgifter ändå inte vara tillåten om sådan behandling exempelvis inte är nödvändig i förhållande till det angivna ändamålet.[161] Vidare innebär samtycke ett uttryck för den enskildes autonomi och självbestämmande, dock endast om alla krav för ett giltigt samtycke är uppfyllda samt att det används i rätt kontext.[162]

EDPB uttrycker att samtycke endast är en lämplig laglig grund om den registrerade kan utöva verklig kontroll över sina personuppgifter och har ett reellt val huruvida personen vill acceptera eller avböja villkoren för samtycket. Vid en begäran om samtycke ligger ansvaret på den personuppgiftsansvarige att bedöma om ett sådant samtycke faktiskt skulle möta kraven i dataskyddsförordningen för att vara ett giltigt samtycke. Om ett samtycke möter alla krav i förordningen uppger EDPB att samtycke som laglig grund är ett verktyg som ger den registrerade kontroll över huruvida personuppgifter rörande personen ska behandlas eller inte. Skulle ett sådant samtycke i realiteten dock inte möta alla uppställda krav innebär ett givande av samtycke i stället att den registrerade upplever en illusorisk känsla av kontroll. Det skulle resultera i att den enskildes ställning i praktiken försvagas, tvärtemot dataskyddsförordningens syfte. Det skulle vidare innebära att samtycket inte kan tillämpas som laglig grund för behandling av personuppgifter eftersom det inte skulle vara ett giltigt sådant. Behandlingen skulle således bli otillåten.[163] Som förstås är det alltså av stor vikt att IoT-företag dels följer, dels har en faktisk möjlighet att följa, de krav på giltigt samtycke som ställs upp i förordningen. Detta både för att inte invagga den registrerade i en falsk känsla av kontroll samt för att det annars skulle innebära att behandlingen av personuppgifterna skulle vara olaglig.

[160] Art. 4.11 dataskyddsförordningen.
[161] EDPB Guidelines 05/2020, s. 5.
[162] WP 187, s. 10 och 33.
[163] EDPB Guidelines 05/2020, s. 5; WP 187, s. 10.

Vidare finns det inget formkrav på hur samtycket ska lämnas utan kan alltså lämnas både skriftligt, inklusive elektroniskt, och muntligt.[164] Dataskyddsförordningen stipulerar dock att det vilar en bevisbörda på den personuppgiftsansvarige att kunna visa att den enskilde har givit sitt samtycke till behandling av sina personuppgifter. [165] Med tanke på detta är det därför lämpligt med skriftligt samtycke trots att det inte föreligger något formkrav. Vidare måste samtycket inhämtas innan behandlingen av personuppgifterna påbörjas.[166]

4.2 Kriterier för giltigt samtycke

4.2.1 Inledning

För att kunna utföra en grundlig analys om hur väl dataskyddsförordningens lagliga grund samtycke är lämpad för IoT krävs en djupare förståelse för de ovan framlagda kriterier som definierar ett giltigt samtycke. Som nämndes är dessa fyra kriterier att ett samtycke ska vara en frivillig, specifik, informerad och en otvetydig viljeyttring.

4.2.2 Frivilligt

4.2.2.1 Inledning

Det första kriteriet för att ett samtycke ska kunna anses vara giltigt är alltså att samtycket lämnats frivilligt av den enskilde.[167] Enligt EDPB innebär frivillighet i denna kontext att den registrerade måste ha ett verkligt val, utan att känna sig tvingad eller pressad att samtycka eller att ett avstående från att samtycka skulle medföra negativa konsekvenser. I ett sådant fall skulle samtycket inte anses vara frivilligt och därmed inte giltigt.[168] Dataskyddsförordningen föreskriver exempelvis att det vid bedömningen av om ett samtycke är frivilligt givet bland annat ska tas hänsyn till huruvida genomförandet av ett avtal har gjorts beroende av att den enskilde samtycker till behandling av sina personuppgifter, trots att sådan behandling inte är nödvändig för genomförandet av avtalet.[169] En närmre diskussion kring detta förs nedan. I artikeln används alltså uttrycket ”bland annat”, vilket indikerar att det vid bedömningen av om ett samtycke är frivilligt givet även ska tas hänsyn till andra situationer. EDPB menar att detta generellt innebär att alla typer av olämplig påtryckning eller påverkan på den registrerade, som medför att den registrerade hindras från att utöva sin fria vilja, ska innebära ett ogiltigt samtycke.[170] Samtycke anses inte heller som frivilligt givet om den registrerade inte har möjlighet att vägra eller återkalla sitt samtycke utan att det skulle

[164] Frydlinger m.fl. (2018), s. 148; skäl 32 dataskyddsförordningen.
[165] Art. 7.1 dataskyddsförordningen.
[166] NJA 2005 s. 361.
[167] Art. 4.11 dataskyddsförordningen.
[168] EDPB Guidelines 05/2020, s. 7 och 9.
[169] Art. 7.4 dataskyddsförordningen.
[170] EDPB Guidelines 05/2020, s. 7-8.

innebära en nackdel för den registrerade. Vidare ska även en eventuell maktobalans mellan den personuppgiftsansvarige och den registrerade beaktas vid bedömningen om samtycket är frivilligt givet.[171] Dessa olika aspekter, som bör undersökas vid bedömningen om ett samtycke kan anses vara frivilligt givet, beskrivs närmre i det följande.

4.2.2.2 Villkorande och granularitet

Som nämnts ovan föreskriver dataskyddsförordningen att det vid bedömningen av om ett samtycke är frivilligt ska tas största hänsyn bland annat till om genomförandet av ett avtal gjorts beroende av att den enskilde samtycker till behandling av personuppgifter som inte är nödvändig för att genomföra avtalet.[172] Med andra ord; om genomförandet av avtalet är villkorat av att den enskilde ger sitt samtycke till behandling av sina personuppgifter som inte är nödvändig. EDPB nämner som exempel på en sådan situation då en bank, för att få tillgång till deras banktjänster, begär samtycke till behandling av den enskildes personuppgifter för att låta tredje part använda dessa i marknadsföringssyften. I en sådan situation är behandlingen av personuppgifter inte nödvändig för genomförandet av banktjänsten. Skulle den enskilde lida nackdelar av att inte ge sådant samtycke, exempelvis att den enskilde inte får tillgång till banktjänsten eller får en höjd avgift, kan det inte anses att ett eventuellt samtycke kan ges frivilligt.[173] Vad som är ”nödvändigt för genomförandet av avtalet” ska enligt EDPB tolkas strikt. EDPB menar dock att det exempelvis kan vara nödvändigt att behandla den enskildes adress för att leverera en vara efter köp via internet eller att behandla betalkortuppgifter för att kunna genomföra ett köp.[174]

Om behandling av personuppgifter faktiskt är nödvändigt för genomförandet av avtalet innebär det inte något hinder för den enskildes fria vilja.[175] I ett sådant fall bör behandlingen av personuppgifter dock heller inte baseras på den lagliga grunden samtycke, utan på nödvändighet på grund av avtal.[176]

Då en behandling av personuppgifter utförs för flera olika ändamål måste vidare samtycke ges för var och ett av ändamålen som stöds på samtycke och inte någon annan laglig grund.[177] Den registrerade ska alltså ha möjlighet att fritt välja för vilka av ändamålen behandling av den registrerades personuppgifter ska få utföras. Det kan alltså krävas flera olika samtycken för att den personuppgiftsansvarige ska kunna erbjuda en tjänst.[178] Om den registrerade inte ges möjlighet att ge separata samtycken för olika ändamål där sådant tillvägagångssätt är lämpligt, utan istället måste samtycka till ett

[171] WP 259, ”Guidelines on consent under Regulation 2016/679”, s. 5.
[172] Art. 7.4 samt skäl 43 dataskyddsförordningen.
[173] EDPB Guidelines 05/2020, s. 11.
[174] EDPB Guidelines 05/2020, s. 10.
[175] EDPB Guidelines 05/2020, s. 11.
[176] Jfr. art. 6.1(b) dataskyddsförordningen.
[177] Skäl 32 dataskyddsförordningen; EDPB Guidelines 05/2020, s. 12.
[178] EDPB Guidelines 05/2020, s. 12.

paket av ändamål, uppger skälen till förordningen att det ska antas att samtycket inte är frivilligt givet.[179] Detta krav på granularitet är nära sammankopplat med kriteriet att ett samtycke måste vara specifikt för att anses giltigt, vilket beskrivs närmre i delavsnitt 4.2.3 nedan.

4.2.2.3 Återkallande av samtycke

Vidare, för att ett samtycke ska anses vara frivilligt, måste den registrerade ha rätt att när som helst återkalla sitt samtycke. Om den registrerade inte kan göra genuina och fria val genom att återkalla ett tidigare givet samtycke kan det inte anses vara frivilligt. Den registrerade måste även, innan samtycke ges, bli informerad om sin rätt att senare kunna återkalla sitt samtycke. Därutöver måste samtycket kunna återkallas lika lätt som det är att ge det.[180]

Dataskyddsförordningen föreskriver inte att en återkallelse av samtycke alltid måste kunna göras genom samma handling. EDPB menar dock att om samtycke är inhämtat via elektroniska medel, såsom musklick, en svepning eller en tangenttryckning, måste samtycket kunna återkallas på ett lika enkelt sätt. EDPB ger som exempel att då samtycke kan ges via en hemsida genom ett musklick är det inte i enlighet med dataskyddsförordnigen om den registrerade därefter, för att återkalla sitt samtycke, måste ringa kundtjänst på arbetsdagar mellan kl. 8-17. Att i ett sådant fall behöva ringa kundtjänst under kontorstid är mer betungande än det musklick som krävdes för att ge sitt samtycke, som dessutom kan göras när som helst. EDPB menar även att om samtycket är inhämtat via exempelvis en app eller via gränssnittet för ett IoT-objekt är det tveklöst att den registrerade måste kunna återkalla samtycket via samma elektroniska gränssnitt. Detta eftersom att behöva återkalla samtycket via ett annat gränssnitt skulle kräva otillbörliga ansträngningar.[181] Dessutom måste den registrerade kunna återkalla samtycket utan att den registrerade lider några nackdelar. Återkallande av sitt samtycke måste alltså bland annat kunna göras avgiftsfritt och utan att servicenivån försämras.[182] Att den registrerade inte ska lida några nackdelar innebär dock inte ett förbud mot att den registrerade kan gå miste om förmåner. Ett sådant fall skulle exempelvis vara då ett IoT-företag erbjuder ett rabatterat pris i utbyte mot kundens samtycke att behandla personens uppgifter för direktmarknadsföring.[183]

Om den registrerade skulle återkalla sitt samtycke förblir all tidigare behandling av personuppgifter som skett med stöd i samtycket laglig.[184] Sådan personuppgiftsbehandling får dock självfallet inte fortskridas efter att samtycket återkallats. Om ingen av de andra lagliga grunderna för behandling i

[179] Skäl 43 dataskyddsförordningen.
[180] Art. 7.3 samt skäl 42 dataskyddsförordningen.
[181] EDPB Guidelines 05/2020, s. 23-24.
[182] EDPB Guidelines 05/2020, s. 24.
[183] Krzysztofek (2021), s. 80.
[184] Art. 7.3 dataskyddsförordningen.

artikel 6 är tillämpliga för vidare behandling måste all insamlad data som skett med stöd i samtycket raderas.[185]

Eftersom IoT-objekt förlorar sitt funktionella värde om det inte kan samla in data som behövs för att det ska fungera ändamålsenligt är dock möjligheten att avstå från tjänster och funktioner mer ett teoretiskt koncept än ett verkligt sådant. Det kan i sådant fall ifrågasättas huruvida konsumentens samtycke faktiskt kan anses vara frivilligt och därmed giltigt, en tanke som även förs upp av artikel 29-gruppen.[186]

4.2.2.4 Maktobalans

Ett samtycke bör inte heller anses vara frivilligt givet i situationer då det råder betydande ojämlikhet mellan parterna. Skälen till dataskyddsförordningen nämner särskilt att det i situationen då ena parten är en offentlig myndighet råder sådan betydande ojämlikhet att ett samtycke inte bör anses vara frivilligt givet av den enskilde.[187] EDPB nämner att det även i situationen arbetsgivare/arbetstagare förekommer sådan betydande ojämlikhet att det är osannolikt att den anställde har möjlighet att neka samtycke till personuppgiftsbehandling utan att uppleva rädsla eller verklig risk för negativa konsekvenser.[188] Givet uttrycket att ett samtycke inte ”bör” anses vara frivilligt i sådana situationer råder alltså inget absolut förbud mot att stödja personuppgiftsbehandlingen på samtycke. Det bör snarare förstås som att en bedömning måste göras utifrån varje enskilt fall.

Då denna uppsats fokuserar på IoT-företag som är privata sådana, och alltså inte är offentliga myndigheter, kommer ingen närmre diskussion kring den relationen att göras. Detsamma gäller med situationen arbetsgivare/arbetstagare då en sådan kontext uppenbarligen inte är fallet vid konsumenters köp och användning av IoT-objekt. Frågan kan dock ställas om det kan tänkas föreligga en likartad maktobalans i förhållandet mellan konsument och IoT-företag som skulle kunna föranleda att ett samtycke inte bör anses vara frivilligt givet. Det finns ju konsumentskyddslagstiftning[189] med särskilt konsumentskyddande regler som erkänner att det finns en maktobalans mellan konsumenter och näringsidkare. Den maktobalans som åsyftas i förhållandet mellan offentlig verksamhet/enskild samt arbetsgivare/arbetstagare är dock sådan att den svagare parten riskerar, eller åtminstone kan ha en berättigad oro över, att den skulle lida betydande men av att inte samtycka. En sådan risk eller oro skulle exempelvis kunna tänkas utgöras av att den enskilde får sämre service gällande, eller helt berövas, rättigheter från staten som denne har rätt till eller att personen kommer utsättas för repressalier på arbetsplatsen. I ett sådant fall är det uppenbart att

[185] EDPB Guidelines 05/2020, s. 24.
[186] Jfr. WP 223, s. 7.
[187] Skäl 43 dataskyddsförordningen.
[188] EDPB Guidelines 05/2020, s. 9.
[189] Se exempelvis konsumentköplag (2022:260).

ett eventuellt samtycke sannolikt inte utgörs av ett helt genuint och fritt val. I relationen mellan konsument/IoT-företag (näringsidkare) kan det dock inte sägas föreligga risk eller berättigad oro hos konsumenten för negativa konsekvenser av samma slag. Om konsumenten exempelvis köper ett uppkopplat kylskåp eller ett hälsoarmband föreligger inte samma potentiella risk för betydande men om konsumenten gentemot företaget väljer att inte samtycka till den personuppgiftsbehandling som begärs. Det enda som då händer är att företaget inte kan behandla den data som är nödvändig för ändamålet, vilket inte resulterar i annat än att objektets funktionalitet troligen går förlorad. Konsumenten bör i en sådan situation inte uppleva någon press, tvång eller risk för andra negativa konsekvenser, som kan vara i fallet då motparten är en offentlig myndighet eller en arbetsgivare. Det kan således konstateras att det inte bör uppstå hinder för den enskildes fria vilja med grund i den maktobalans som i andra fall anses föreligga mellan en konsument och en näringsidkare.

4.2.3 Specifikt

4.2.3.1 Inledning

Som stipuleras i dataskyddsförordningen måste ett samtycke lämnas för ett eller flera specifika ändamål för att vara giltigt.[190] Ett generellt samtycke för ett paket av ändamål är således inte specifikt. Syftet med regeln är att bidra till den registrerades kontroll och transparensen av hur och vilka personuppgifter som behandlas.[191] EDPB menar att för att ett samtycke ska anses vara specifikt måste tre element uppfyllas; ändamålsspecificering, granularitet och särskiljande av information.[192] Dessa ska således beskrivas närmre nedan.

Kravet på att samtycket måste lämnas för specifika ändamål är tätt sammankopplat med i delavsnitt 4.2.3.3 ovan beskrivna krav på granularitet för att ett samtycke ska kunna anses vara frivilligt givet. Det hänger även nära samman med kravet på att ett samtycke ska vara informerat för att vara giltigt, vilket beskrivs närmre nedan i delavsnitt 4.2.4.[193] På grund av dessa nära kopplingar till andra kriterier kommer detta avsnitt att hållas relativt kort.

4.2.3.2 Ändamålsspecificering

Som beskrivits tidigare i delavsnitt 3.5.1 ska hela dataskyddsförordningen genomsyras bland annat av principen om ändamålsbegränsning, vilket även gäller reglerna för ett giltigt samtycke. Som framkommer genom bestämmelsen måste ett samtycke alltid föregås av ett specificerat ändamål, som

[190] Art. 6.1(a) dataskyddsförordningen.
[191] EDPB Guidelines 05/2020, s. 14.
[192] EDPB Guidelines 05/2020, s. 14.
[193] EDPB Guidelines 05/2020, s. 13-14.

måste vara särskilt, uttryckligt angivet och berättigat.[194] Ett generellt samtycke till behandling av personuppgifter är alltså inte specifikt, utan samtycket måste avse den exakta berörda personuppgiftsbehandlingen.[195] Kravet på att ett samtycke ska vara specifikt tillsammans med kravet om ändamålsbegränsning syftar till att motverka att ändamålet för vilket personuppgiftsbehandlingen sker efter hand vidgas eller suddas ut. Detta kallas även för ändamålsglidning, något som kan göra att den enskildes personuppgifter används på ett oväntat sätt och minskar den enskildes kontroll.[196] Bland annat menar artikel 29-gruppen, som tidigare framgått i delavsnitt 3.5.3, att ett vagt och allmänt angivet ändamål, såsom ”förbättring av användarupplevelsen”, ”marknadsföringssyften” eller ”för framtida forskning” troligen inte skulle möta kravet på ett specifikt angivet ändamål.[197]

4.2.3.3 Granularitet

Granularitet gäller inte enbart för att ett samtycke ska kunna anses vara frivilligt, utan även för att det ska vara ett specifikt sådant. När den personuppgiftsansvarige begär samtycke för flera olika ändamål måste den registrerade alltså ha möjlighet att ge specifikt samtycke till var och ett av ändamålen.[198]

4.2.3.4 Särskiljande av information

För att ett samtycke ska anses vara specifikt måste slutligen den registrerade få specificerad information om varje ändamål det begärs samtycke för. Detta för att den registrerade ska göras medveten om vilka olika möjligheter den registrerade har och således kunna ge ett specificerat samtycke.[199] Kravet på information som särskiljer varje ändamål för att ett samtycke ska anses vara specifikt hänger tätt samman med kravet på att den personuppgiftsansvarige generellt måste ge klar och tydlig information för att ett samtycke ska anses vara giltigt. Detta beskrivs närmre i det följande.

4.2.4 Informerat

4.2.4.1 Inledning

Dataskyddsförordningen stipulerar att ett giltigt samtycke måste vara informerat.[200] Att ett samtycke ska vara informerat innebär att den registrerade ska ha nödvändig information till sitt förfogande innan någon behandling av personuppgifter sker och därmed innan personen fattar ett beslut om samtycke.[201] Den registrerade måste göras medveten om vad det är personen

[194] Se art. 5.1(b) dataskyddsförordningen.
[195] Se mål C-61/19 *Orange România*, EU:C:2020:901, punkt 38; Öman (2021), s. 101.
[196] EDPB Guidelines 05/2020, s. 14.
[197] WP 203, s. 15-16.
[198] EDPB Guidelines 05/2020, s. 14.
[199] EDPB Guidelines 05/2020, s. 15.
[200] Art. 4.11 dataskyddsförordningen.
[201] WP 202, ”Opinion 02/2013 on apps on smart devices”, s. 15 och 22.

samtycker till och till exempel om rätten att återkalla sitt samtycke, som tidigare beskrivits i delavsnitt 4.2.2.3.[202] Att ett samtycke är informerat krävs för att uppfylla den fundamentala principen om att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade. Det är även nära sammankopplat med principerna om korrekthet (fairness) och laglighet.[203] Om den registrerade inte ges tillräcklig information för att förstå vad den samtycker till blir den upplevda kontrollen i stället endast en illusorisk sådan och samtycket blir en ogiltig grund för behandling.[204]

I dataskyddsförordningen uppställs krav på viss information som måste delges den registrerade vid behandling av personuppgifter för att den personuppgiftsansvarige ska agera i enlighet med förordningen.[205] Dessa gäller dock generellt och är alltså tillämpliga oavsett vilken laglig grund för behandling den personuppgiftsansvarige väljer att stödja personuppgiftsbehandlingen på. Dessa särskilda krav på information är alltså inte kopplade specifikt till den lagliga grunden samtycke. EDPB är av åsikten att de generella informationskraven och kraven för att uppfylla ett informerat samtycke i praktiken bör leda till ett integrerat tillvägagångssätt i många fall. EDPB menar dock att kraven för ett informerat samtycke kan uppfyllas även om inte alla delar i de generella informationskraven nämns vid erhållandet av ett samtycke.[206] Det betyder att det enligt EDPB:s synsätt kan föreligga ett informerat samtycke trots att den personuppgiftsansvariges agerande kan strida mot förordningen avseende de generella informationskraven. Med hänvisning till EDPB:s betydelse för tolkningen av dataskyddsförordningen, som framgår i avsnitt 1.3 om metod och material, väljer jag att utgå från EDPB:s uttalande. Vid den vidare utredningen av dataskyddsförordningens krav på samtycke utesluts därför de informationskrav som inte anses krävas för att erhålla ett informerat och giltigt samtycke.

4.2.4.2 Vilken information som ska ges

För att ett samtycke ska anses vara informerat föreskrivs i skälen till dataskyddsförordningen att den registrerade bör göras medveten om åtminstone den personuppgiftsansvariges identitet och syftet med personuppgiftsbehandlingen.[207] Någon ytterligare klar vägledning om vad den registrerade ska informeras om för att ett samtycke ska anses vara informerat och därmed giltigt saknas i dataskyddsförordningen. EDPB listar dock ett antal krav den anser vara särskilt viktiga, som en slags miniminivå, rörande vad informationen ska innehålla för att den registrerade därefter ska kunna anses ge ett informerat samtycke. Dessa minimikrav är att den registrerade ska informeras om:

[202] EDPB Guidelines 05/2020, s. 15.
[203] Jfr. art. 5 dataskyddsförordningen; EDPB Guidelines 05/2020, s. 15.
[204] EDPB Guidelines 05/2020, s. 15.
[205] Se framför allt art. 13 och 14 dataskyddsförordningen.
[206] EDPB Guidelines 05/2020, s. 17.
[207] Skäl 42 dataskyddsförordningen.

- Den personuppgiftsansvariges identitet
- Syftet med varje personuppgiftsbehandling det begärs samtycke för
- Vilken typ av data som kommer behandlas
- Den registrerades rättighet att återkalla sitt samtycke
- Om insamlad data kommer användas för automatiserat beslutsfattande, samt
- Om det finns risk för överföring av personuppgifter där lämpliga skyddsåtgärder saknas[208]

EDPB uttalar dock att det med hänvisning till omständigheterna i varje enskilt fall kan krävas att den registrerade ges mer information för att den registrerade genuint ska förstå hur personens personuppgifter kommer behandlas och därmed för att ett samtycke ska anses vara informerat.[209] Som framkommit genom EU-domstolens praxis krävs det att den registrerade har möjlighet att avgöra följderna av ett samtycke.[210]

Skulle ändamålet med behandlingen ändras måste den personuppgiftsansvarige erhålla nytt samtycke från den registrerade. Den personuppgiftsansvarige måste då tillhandahålla den registrerade information om det nya ändamålet för att den registrerade ska kunna göra ett informerat beslut.[211] Liknande måste ett nytt samtycke inhämtas om den personuppgiftsansvarige väljer att behandla personuppgifterna på ett annat sätt än det sätt som den registrerade ursprungligen givit samtycke till.[212]

4.2.4.3 Hur information ska ges

Den personuppgiftsansvarige måste utvärdera vilken typ av målgrupp den riktar sig till innan den behandlar enskildas personuppgifter för att kunna bedöma exempelvis vilket typ av språk som bör användas. EDPB ger som exempel att om målgruppen är minderåriga måste informationen vara förståelig för minderåriga. När den personuppgiftsansvarige har identifierat målgruppen måste den personuppgiftsansvarige därefter avgöra vilken information som ska ges och hur informationen ska presenteras för den registrerade.[213]

Likt vid givande av samtycke föreskriver inte dataskyddsförordningen i vilken form information ska ges till den registrerade för att ett samtycke ska anses vara informerat och därmed giltigt. Det innebär att det finns möjlighet att lämna informationen på flera olika sätt, såsom skriftligen, muntligen eller via röst- eller videosamtal.[214] Förordningen stipulerar dock krav gällande

[208] EDPB Guidelines 05/2020, s. 15-16.
[209] EDPB Guidelines 05/2020, s. 16.
[210] EU-domstolens dom, *Orange România*, C-61/19, punkt 40.
[211] WP 187, s. 19.
[212] Jämför Datainspektionens rapport 2002:4, s. 13.
[213] EDPB Guidelines 05/2020, s. 16-17.
[214] EDPB Guidelines 05/2020, s. 16.

informationens tydlighet och tillgänglighet. För att uppfylla öppenhetsprincipen föreskriver exempelvis skälen till dataskyddsförordningen att all information och kommunikation som är relaterat till personuppgiftsbehandlingen ska ske på ett lättillgängligt och lättbegripligt sätt samt att ett klart och tydligt språk ska användas.[215] Vidare stipulerar förordningen ett tydlighetskrav i de fall samtycket ska lämnas i en skriftlig förklaring som även innehåller andra frågor. Ett exempel på ett sådant fall är om den registrerade på samma gång ska godkänna avtalsvillkor. Då ska begäran om samtycke gällande behandling av personuppgifter framställas på ett sätt som klart och tydligt särskiljer samtyckesbegäran från de övriga frågorna, i en begriplig och lättillgänglig form. Vidare föreskrivs det även här att det ska användas ett klart och tydligt språk.[216] Som EDPB skriver måste den personuppgiftsansvarige alltså se till att ett klart och tydligt språk alltid används. Det innebär att informationen lätt ska kunna förstås av gemene man och inte endast av jurister. Det medför att begäran om samtycke inte får lämnas i meddelanden fulla av juridisk jargong i långa integritetspolicyer som är svåra att förstå, eftersom en sådan begäran varken skulle vara lättförståelig eller skild från övrig information.[217]

Vidare stipulerar skälen till dataskyddsförordningen att då samtycket ska ges elektroniskt måste begäran om sådant samtycke vara tydlig och koncis.[218] För att uppfylla dataskyddsförordningens krav om å ena sidan exakthet och fullständighet och å andra sidan begriplighet menar EDPB att ett lämpligt tillvägagångssätt kan vara att lämna informationen på ett skiktat och granulärt sätt.[219] Med det får förstås att det kan vara lämpligt att tillhandahålla informationen i olika etapper och att informationen är specifik i förhållande till vad den ska förmedla.

Som framkom genom kommissionens undersökning gällande dataskyddsförordningen år 2019 var det 47 % av respondenterna som uppgav att de delvis läste integritetspolicys online och endast 13 % som läste dem fullständigt. Vidare uppgav 37 % att de inte läste integritetspolicys online över huvud taget. Vid en jämförelse med kommissionens föregående undersökning år 2015 framgår att EU-befolkningen år 2019 generellt var mindre benägna att delvis eller fullständigt läsa integritetspolicys online.[220] Vid frågan varför respondenterna endast delvis eller inte alls läser integritetspolicys

[215] Skäl 39 dataskyddsförordningen.
[216] Art. 7.2 dataskyddsförordningen; Frydlinger m.fl. (2018), s. 148.
[217] EDPB Guidelines 05/2020, s. 16.
[218] Skäl 32 dataskyddsförordningen.
[219] EDPB Guidelines 05/2020, s. 17.
[220] Europeiska kommissionen, Special Eurobarometer 487a: The General Data Protection Regulation, (2019), s. 47.

svarade en majoritet på 66 % att de är för långa. Vidare ansåg 31 % att de var oklara och svåra att förstå.[221]

Värt att notera är att kommissionens undersökning alltså handlar om integritetspolicys och inte enbart information just vid begäran om samtycke, som denna uppsats är fokuserad kring. Resultatet som framkommit genom undersökningen bör dock kunna appliceras även på information vid begäran om samtycke. Detta då en samtyckesbegäran kan vara en del av den information gällande den enskildes integritet som krävs för att den enskilde ska kunna utöva full kontroll över sina personuppgifter. Det gäller även i stora drag samma typ av information.

Genom undersökningen framgår det alltså att det föreligger en diskrepans mellan den skrivna rätten och utfallet i verkligheten. Detta syns då en majoritet inte läser integritetspolicys på grund av att de är för långa, vilket motverkar syftet med förordningen, nämligen att all information ska vara lättillgänglig och lättbegriplig. Vidare syns det genom att en tredjedel av respondenterna anser att integritetspolicyerna är oklara och svåra att förstå trots att dataskyddsförordningen kräver att all information är lättbegriplig och att ett klart och tydligt språk används. Det brister således i öppenhetsprincipen. Att det är en mindre andel respondenter som uppger sig läsa integritetspolicys år 2019 jämfört med år 2015 skulle kunna bero på att befolkningen tröttnat på den ansenliga mängd information gällande deras personliga data som enskilda nästintill dagligen möts av.

4.2.5 Otvetydig viljeyttring

4.2.5.1 Inledning

Det fjärde och sista villkoret för att ett samtycke ska anses vara ett giltigt sådant är att den enskilde godtar behandlingen av sina personuppgifter genom en otvetydig viljeyttring.[222] Som artikel 29-gruppen skriver får det inte föreligga några tvivel gällande den registrerades avsikt att ge sitt samtycke. Finns det några som helst tvivel gällande vad som är eller har varit den registrerades avsikt föreligger det tvetydighet.[223] I ett sådant fall har den enskilde inte gett en otvetydig viljeyttring och ett eventuellt samtycke skulle inte vara giltigt.

4.2.5.2 Genom ett uttalande eller en entydig bekräftande handling

Enligt dataskyddsförordningen måste den otvetydiga viljeyttringen om att godta behandlingen av sina personuppgifter ske genom ett uttalande eller

[221] Europeiska kommissionen, Special Eurobarometer 487a: The General Data Protection Regulation, (2019), s. 51.
[222] Art. 4.11 dataskyddsförordningen.
[223] WP 187, s. 21.

genom en entydig bekräftande handling.[224] Med en entydig bekräftande handling menas att den registrerade måste ha utfört en avsiktlig handling för att samtycka till personuppgiftsbehandlingen.[225] Samtycket måste alltså ges aktivt eller genom en förklaring för att det ska vara uppenbart att den registrerade har samtyckt till behandlingen.[226] I skälen till förordningen skrivs att den registrerades tystnad eller inaktivitet därför inte bör betraktas som ett aktivt val och bör således inte utgöra ett giltigt samtycke. På samma sätt anges i skälen att på förhand ikryssade rutor inte heller bör utgöra ett giltigt samtycke.[227] Vidare anger EDPB att endast att scrolla genom en hemsida eller fortsätta med en tjänst inte heller uppfyller kraven på en entydig bekräftande handling. Detta då sådana handlingar kan vara svåra att skilja från annan aktivitet eller interaktion av en användare. Vidare skulle det i ett sådant fall vara svårt att tillhandahålla ett sätt för användaren att återkalla samtycke på ett sätt som är lika lätt som det var att ursprungligen ge samtycket.[228] Återkallande av samtycke diskuterades tidigare i delavsnitt 4.2.2.3 gällande frivilligt givande av samtycke. Tystnad eller inaktivitet skulle många gånger också innebära svårigheter för den personuppgiftsansvarige att bevisa att denne erhållit ett giltigt samtycke. Dessutom kan ett giltigt samtycke, som tidigare nämnts i delavsnitt 4.2.4.3, inte erhållas på samma gång och på samma sätt som den registrerade godtar ett avtal eller allmänna villkor för en viss tjänst. Detta för att ett sådant godkännande av allmänna villkor inte kan ses som en entydig bekräftande handling om att samtycka till behandling av personuppgifter.[229]

4.2.5.3 Hur samtycke kan ges

I skälen till dataskyddsförordningen föreskrivs, som ovan nämnts, att samtycke kan lämnas genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Som exempel på hur ett giltigt samtycke kan ges tas upp att personen vid besök på en internetsida aktivt kan kryssa i en ruta. Personen skulle också kunna ställa in inställningar för tjänster på informationssamhällets område, eller genom annan förklaring eller beteende tydligt visa att den enskilde godtar behandling av personuppgifter som rör denne.[230] Öman menar att det genom den beskrivningen framgår att även konkludent handlande utgör en entydig bekräftande handling och kan därmed anses utgöra en otvetydig viljeyttring. Ett exempel på ett sådant konkludent handlande skulle kunna vara om den registrerade lämnar de personuppgifter som efterfrågas. Dock krävs det att personen dessförinnan tillhandahållits information om behandlingen, om att det är frivilligt att lämna personuppgifter samt att

[224] Art. 4.11 dataskyddsförordningen.
[225] EDPB Guidelines 05/2020, s. 18.
[226] EDPB Guidelines 05/2020, s. 18; se även mål C-673/17 *Planet49*, EU:C:2019:801, punkt 62, samt mål C-61/19 *Orange România*, EU:C:2020:901, punkt 35.
[227] Skäl 32 dataskyddsförordningen.
[228] EDPB Guidelines 05/2020, s. 18-19.
[229] EDPB Guidelines 05/2020, s. 18-19.
[230] Skäl 32 dataskyddsförordningen.

det betraktas som ett samtycke om man väljer att uppge sina personuppgifter.[231]

Vidare föreskriver skälen att när det gäller en elektronisk begäran om samtycke får begäran inte i onödig mån störa användningen av tjänsten som samtycket avser.[232] EDPB uttalar dock att en aktiv handling genom vilken den registrerade samtycker till behandling kan vara nödvändig om ett mindre ingripande eller störande tillvägagångssätt skulle resultera i tvetydighet. EDPB anser att det därför kan vara nödvändigt att en begäran om samtycke stör användarupplevelsen i viss mån för att begäran om samtycke ska bli tydlig och ändamålsenlig. Så länge den dataskyddsansvarige följer dataskyddsförordningen menar EDPB att den personuppgiftsansvarige kan utveckla egna sätt att inhämta samtycke på som lämpar sig för just deras organisation. Som exempel nämner EDPB att samtycke kan ges genom att den registrerade viftar framför en smartkamera eller vrider en smarttelefon medurs eller i en åtta. Det viktiga är att handlingen otvetydigt visar att åtgärden innebär att den registrerade samtycker till en specifik begäran samt att sådan information som krävs för att ett samtycke ska anses vara informerat ges. Det är dessutom viktigt att den personuppgiftsansvarige kan visa att samtycke har erhållits på sättet i fråga och att den registrerade kan återkalla sitt samtycke lika enkelt som det gavs.[233] Därutöver skriver artikel 29-gruppen att den personuppgiftsansvarige måste vara tillräckligt säker på att den som ger samtycket faktiskt är den registrerade, något som uppges gälla särskilt när samtycke exempelvis ges online.[234]

EDPB nämner även faktumet att det i den digitala verkligheten finns många tjänster som kräver personuppgifter för att fungera ändamålsenligt. Det gör att registrerade får flertalet samtyckesförfrågningar dagligen. När registrerade överexponeras för dessa förfrågningar och ständigt behöver ta ställning och exempelvis klicka eller svajpa för att visa sin vilja minskar varningseffekten av samtycket. Detta kallar EDPB ”klicktrötthet”. Det resulterar i att registrerade slutar läsa informationen rörande samtycket och samtycker för hastigt utan att vara fullt informerade om innebörden av det. Det innebär i sin tur en särskild risk för den registrerade då samtycke som regel efterfrågas för åtgärder som i princip är olagliga utan den registrerades medgivande. Hur denna klicktrötthet ska tacklas är inget som dataskyddsförordningen tar upp, utan det lämnas åt de personuppgiftsansvariga att finna lösningar på detta problem. Som exempel nämner EDPB dock att när det gäller webbplatser skulle en lösning kunna vara att registrerade väljer vad den vill samtycka till i sina webbläsarinställningar, vilket sedan gäller generellt.[235]

[231] Öman (2021), s. 96.
[232] Skäl 32 dataskyddsförordningen.
[233] EDPB Guidelines 05/2020, s. 19.
[234] WP 187, s. 21.
[235] EDPB Guidelines 05/2020, s. 19.

4.3 Känsliga uppgifter

Som nämndes i tidigare delavsnitt 3.3.1 om vad som är personuppgifter innehåller dataskyddsförordningen särskild reglering kring personuppgifter som räknas som känsliga, eller som det i förordningen är kallat; särskilda kategorier av personuppgifter. För att friska upp läsarens minne berör denna reglering uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening. Vidare omfattar den också genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa, sexualliv eller sexuell läggning. Det är som huvudregel förbjudet att behandla sådana typer av personuppgifter.[236] Dessa har alltså givits ett särskilt starkt skydd i dataskyddsförordningen eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna.[237] Förordningen innehåller dock ett antal undantag då behandling av känsliga uppgifter ändå är tillåtet. Ett sådant undantag är när den registrerade uttryckligen givit sitt samtycke till behandlingen.[238] Den personuppgiftsansvarige måste, förutom att ha ett tillämpligt undantag, även kunna stödja behandlingen av de känsliga personuppgifterna i någon av de lagliga grunderna i artikel 6.[239]

Till skillnad från ett vanligt samtycke som kräver ett uttalande eller en entydig bekräftande handling för att vara giltigt så krävs det alltså att ett samtycke gällande känsliga uppgifter är uttryckligt.[240] Kraven på ett samtycke för behandling av känsliga uppgifter är i och med ordet ”uttryckligt” högre ställda än på ett vanligt samtycke.[241] Det finns ingen närmare förklaring i dataskyddsförordningen vad som menas med ett uttryckligen lämnat samtycke. EDPB skriver dock att ordet ”uttryckligt” hänvisar till sättet den registrerade lämnar sitt samtycke. Ett sätt att säkerställa att ett samtycke är uttryckligt menar styrelsen skulle vara att den registrerade bekräftar sitt samtycke i en skriftlig förklaring, med exempelvis en underskrift av den registrerade. I digitala eller internetrelaterade sammanhang skulle ett uttryckligt samtycke kunna ges genom att den registrerade fyller i ett elektroniskt formulär, skickar ett e-postmeddelande, laddar upp ett skannat dokument med den registrerades underskrift eller genom att använda elektronisk underskrift. Den registrerade skulle också kunna ge ett uttryckligt samtycke genom att klicka i Ja/Nej-rutor, förutsatt att det tydligt framgår att det är ett samtycke.

[236] Art. 9.1 och 9.2(a) dataskyddsförordningen.

[237] Skäl 51 dataskyddsförordningen; EDPB Guidelines 05/2020, s. 20.

[238] Art. 9.2(a) dataskyddsförordningen; Dataskyddsförordningen ger dock EU-rätten och medlemsstaterna möjlighet att föreskriva att huvudregeln om att behandling av känsliga uppgifter är förbjuden inte ska kunna upphävas av den registrerade, se art. 9.2(a) dataskyddsförordningen.

[239] Kuner m.fl. (2020), s. 376.

[240] Art. 9.2(a) dataskyddsförordningen.

[241] Wendleby och Wetterberg (2019), s. 90.

Den registrerade skulle också kunna uttryckligt samtycka till behandlingen av känsliga uppgifter genom en tvåstegsverifiering. Den registrerade skulle i ett sådant fall kunna få ett e-postmeddelande från den personuppgiftsansvarige med en begäran om samtycke för behandling av känsliga uppgifter som den registrerade måste svara på innehållande orden ”Jag samtycker”. När svaret är skickat skulle därefter den registrerade kunna få en verifieringslänk denne måste klicka på, eller ett sms med en verifieringskod, för att bekräfta sitt samtycke. EDPB menar vidare att även en muntlig förklaring kan utgöra ett giltigt uttryckligt samtycke. Det kan dock i de fallen vara svårt för den personuppgiftsansvarige att bevisa att alla villkor för ett giltigt uttryckligt samtycke var uppfyllda när den muntliga förklaringen spelades in.[242]

De olika kraven på samtycke för vanliga personuppgifter och för känsliga personuppgifter, det vill säga genom ett uttalande eller en entydig bekräftande handling respektive ett uttryckligen lämnat samtycke, kan tyckas något oklara. Ett samtycke är ju lämnat eller så är det inte det. Gällande det lägre kravet, för vanliga personuppgifter, krävs det som tidigare framkommit att det är otvetydigt att den registrerade samtycker till behandlingen. Det måste alltså vara utom tvivel att den registrerades avsikt varit att godkänna personuppgiftsbehandlingen avseende de specifika ändamålen. Är samtycket tvetydigt är det inte giltigt. Hur det då kan finnas ett högre ställt krav, där det ska råda ännu mindre tvivel om den enskildes avsikt, är svårbegripligt. Antingen är det utom tvivel att den registrerade har samtyckt till behandlingen eller så är det inte det. Något mellanläge bör inte kunna finnas. Dessutom föreskriver dataskyddsförordningen att samtycke för vanliga personuppgifter måste ges genom en viljeyttring som antingen är ett uttalande eller en entydig bekräftande handling, det vill säga ”uttryckligt”. Vad för egentlig skillnad som därmed åsyftas får anses vara oklart. Öman redogör för en liknande tanke.[243] Frågan uppkommer om det inte i praktiken är så att kravet på att ett samtycke måste vara uttryckligen lämnat främst syftar till att uppmärksamma att personuppgiftsbehandlingen innebär en särskild dataskyddsrisk, men att kravet i praktiken inte innebär någon större materiell skillnad.

De övriga undantagen som kan göra en behandling av känsliga uppgifter tillåten får i huvudsak anses vara otillämpliga i IoT-sammanhang. Dessa undantag gäller bland annat då det är nödvändigt för den personuppgiftsansvarige att utöva skyldigheter eller rättigheter inom arbetsrätten, om den registrerade redan offentliggjort personuppgifterna på ett tydligt sätt eller då det är nödvändigt av hänsyn till ett viktigt allmänt intresse. När det kommer till IoT och behandling av känsliga personuppgifter får det alltså sägas att det i normala fall krävs att IoT-företaget erhåller den registrerades uttryckliga samtycke.

[242] EDPB Guidelines 05/2020, s. 20-21.
[243] Öman (2021), s. 93.

4.4 Profilering och automatiserat beslutsfattande

Vidare behandlar dataskyddsförordningen profilering och automatiserat beslutsfattande. Profilering definieras i dataskyddsförordningen som ”varje form av automatisk behandling av personuppgifter som består i att dessa används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.”[244] Profilering kan enligt artikel 29-gruppen delas in i tre steg; (1) datainsamling, (2) automatiserad analys för att fastställa samband, och (3) tillämpa det funna sambandet på en individ för att identifiera exempelvis särdrag hos nuvarande eller framtida beteenden, intressen eller förmåga att genomföra en uppgift.[245] I relation till vad som tidigare framkom i avsnitt 2.5 om hur insamlad data kan användas är det alltså just profilering IoT-objekt har en tendens att utföra, med hjälp av sensor fusion och big data-analyser.

Automatiserat beslutsfattande definieras inte i dataskyddsförordningen. Däremot skriver artikel 29-gruppen att automatiserat beslutsfattande innebär förmågan att fatta beslut med tekniska medel, utan mänsklig inblandning. Vidare menar arbetsgruppen att automatiserat beslutsfattande omfattar annat än profilering, men kan delvis överlappa med, eller bli resultatet av, profilering.[246]

Som artikel 29-gruppen skriver kan profilering och automatiserat beslutsfattande vara användbart och behjälpligt för enskilda, till exempel genom ökad effektivitet och resursbesparingar. Som framkommit ovan i avsnitt 2.3 kan det i IoT-sammanhang exempelvis handla om optimering av elförbrukningen och minskad elkonsumtion. Det medför dock även risk för enskildas rättigheter och friheter vilket kräver lämpliga skyddsåtgärder. Detta särskilt eftersom, som tidigare framkommit i uppsatsen, enskilda kan ha svårt att förstå hur deras personliga information används i sådana komplexa tekniker eller ens *att* deras information används för att skapa profiler om dem. Att personlig data används på detta sätt för att skapa profiler kan upprätthålla befintliga stereotyper och social segregation samt ”låsa in” dem i specifika kategorier. Detta kan i sin tur underminera deras frihet att göra val utefter sina egna preferenser. Artikel 29-gruppen menar vidare att profilering i vissa fall kan resultera i felaktiga förutsägelser och även nekande av varor och tjänster samt omotiverad diskriminering.[247]

Artikel 29-gruppen skriver fortsättningsvis att profilering potentiellt kan användas på tre sätt; (1) generell profilering, (2) beslutsfattande baserat på

[244] Art. 4.4 dataskyddsförordningen.

[245] WP 251, ”Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, s. 7.

[246] WP 251, s. 8.

[247] WP 251, s. 5-6.

profilering och (3) enbart automatiserat beslutsfattande, inkluderat profilering, som har rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar denne. Skillnaden mellan punkt (2) och (3) kan illustreras med att det under punkt (2) kan vara en människa som tar beslut utifrån en automatiskt skapad profil och under punkt (3) att det är en algoritm som fattar beslut utan meningsfull inblandning av en människa.[248] Med bakgrund av IoT:s natur är det endast de fall då profilering och beslutsfattande sker automatiskt som är relevanta i detta sammanhang.

Inga ytterligare regleringar tillkommer när det gäller ”vanlig” profilering eller automatiserat beslutsfattande. I de fallen krävs det alltså enbart att behandlingen baseras på någon av de lagliga grunderna för behandling, där samtycke utgör en sådan laglig grund, samt följer dataskyddsförordningens grundläggande principer. Om det däremot gäller enbart automatiserat beslutsfattande, inbegripet profilering, ställer dataskyddsförordningen upp särskilda krav, om det har rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar denne.[249] Sådan behandling är som huvudregel förbjuden, vilket framkommer av artikel 22.1 i dataskyddsförordningen.[250]

Dataskyddsförordningen definierar varken ”rättslig följd” eller vad som innebär ”på liknande sätt i betydande grad”. Artikel 29-gruppen menar dock att det är tydligt att det endast är allvarliga effekter som åsyftas. Arbetsgruppen menar att rättsliga följder kan vara att beslutet påverkar den enskildes lagliga rättigheter, såsom associationsfrihet, att rösta i val eller vidta rättsliga åtgärder. Rättsliga följder kan även innebära en påverkan på den enskilde personens juridiska status, exempelvis nekat medborgarskap, eller rättigheter enligt ett avtal.[251]

Artikel 29-gruppen menar vidare att följder som ”på liknande sätt i betydande grad påverkar” denne inkluderar följder som avsevärt påverkar den enskildes omständigheter, beteende eller val, har en långvarig eller permanent inverkan på den enskilde eller leder till uteslutning eller diskriminering av enskilda. På grund av svårigheten att beskriva vad som är tillräckligt allvarligt för att anses vara ”betydande grad” uppställer artikel 29-gruppen ett antal exempel, såsom beslut som påverkar någons finansiella omständigheter som exempelvis deras rätt till kredit, tillgång till hälso- och sjukvård eller beslut som nekar någon en anställningsmöjlighet eller i en sådan situation innebär en betydande nackdel.[252] Som tidigare framkom i avsnitt 2.5 om hur insamlad data kan användas menar Peppet att IoT-tekniken möjliggör för exempelvis banker att bedöma om den enskilde är en god kreditrisk, för

[248] WP 251, s. 8-9.

[249] Jfr. art. 22 dataskyddsförordningen.

[250] Jfr. WP 251 s. 19-20 om argumentation angående varför artikeln bör anses konstituera ett förbud.

[251] WP 251, s. 21.

[252] WP 251, s. 21-22.

arbetsgivare att bedöma om de ska anställa den enskilde eller inte, eller för ett försäkringsbolag att bestämma vilken premie den enskilde ska betala. IoT-objekt kan med andra ord mycket väl innebära att automatiska beslut fattas som i betydande grad påverkar den enskilde på det sätt som åsyftas i dataskyddsförordningen och som huvudregel därmed är förbjuden.

Dataskyddsförordningen uppställer dock undantag då sådan behandling ändå är tillåten. Ett sådant undantag är om det automatiserade beslutet grundar sig på den registrerades uttryckliga samtycke, det vill säga samma rekvisit som när det rör känsliga personuppgifter.[253] Detta eftersom även situationer som faller inom definitionen av automatiserat individuellt beslutsfattande innebär en betydande dataskyddsrisk där det, som artikel 29-gruppen skriver, anses lämpligt att den enskilde innehar en hög nivå av kontroll över sin personliga information. Inte heller i förhållande till automatiserat individuellt beslutsfattande innehåller dataskyddsförordningen en definition av begreppet uttryckligt samtycke. Artikel 29-gruppen hänvisar dock till deras tidigare riktlinjer för samtycke vid tolkning av begreppet, vilka beskrevs i avsnittet ovan om känsliga personuppgifter.[254] Eftersom det handlar om samma rekvisit som är uppställt av samma anledning som vid känsliga uppgifter hänvisas läsaren till ovan förda diskussion om rekvisitet uttryckligt samtycke.

I relation till vad som tidigare skrivits om svårigheterna för enskilda att förstå denna teknik och hur deras personliga information används är det vidare viktigt att den personuppgiftsansvarige kan visa att den registrerade har förstått precis vad det är den samtyckt till. Den enskilde måste alltså förstå logiken bakom profileringen och beslutsfattandet. Det är således viktigt att den registrerade erhåller tillräcklig information om den planerade behandlingen och konsekvenserna av den, för att säkerställa att samtycket utgör ett informerat samtycke.[255]

Som framkommit i förevarande avsnitt, samt i tidigare avsnitt 2.5 om hur insamlad data kan användas, kan IoT-objekt över tid och genom sensor fusion och big data-analyser dra oväntade slutsatser och skapa en större informationsbild om användaren än vad en sensor ensamt kunnat skapa. Det kan resultera i att uppgifter som från början inte tycks vara personuppgifter kan, efter profilering och samkörning med annan insamlad information, slutligen användas för att direkt eller indirekt identifiera en fysisk person och därmed utgöra personuppgifter. Detsamma gäller med uppgifter som från början inte tycks vara av känslig natur, men som efter sådan behandling kan användas för att dra slutsatser som gör att personuppgifterna trots allt bör kvalificeras som känsliga sådana. Exempelvis skulle det kunna vara möjligt

[253] Art. 22.2(c) dataskyddsförordningen.

[254] WP 251, s. 24; riktlinjerna om samtycke som artikel 29-gruppen hänvisar till hittas i WP 259.

[255] WP 251, s. 13.

att dra slutsatser om en persons hälsotillstånd utifrån uppgifter om personens matvaruinköp i kombination med data om livsmedlens kvalitet och energiinnehåll.[256] I ett sådant fall måste den personuppgiftsansvarige se till att kraven både vad gäller känsliga personuppgifter samt automatiserat individuellt beslutsfattande följs. Som framkom i det föregående avsnittet om känsliga uppgifter bör uttryckligt samtycke i princip vara det enda undantag som kan göra en behandling av känsliga uppgifter tillåten i IoT-sammanhang. Således innebär det att även automatiserat individuellt beslutsfattande, inbegripet profilering, som har ovan beskrivna omständigheter till följd och som involverar känsliga personuppgifter endast är tillåtet vid erhållandet av uttryckligt samtycke. Med andra ord bör i de fallen ingen av de övriga undantag som kan göra automatiserat individuellt beslutsfattande tillåtet vara tillämpliga.

[256] WP 251, s. 15.

5 Sammanfattning och avslutande analys

5.1 Inledande sammanfattning

Vi är redan vana vid att ha smarta hälsoarmband på våra handleder, elektroniska larm i våra hem som kan styras på avstånd och smarta röstassistenter som kan utföra olika åtgärder, som att sätta på en lampa eller besvara en nyss påkommen fråga. Det kan inte sägas annat än att IoT-objekten redan har revolutionerat våra liv och att de är här för att stanna. Som framkommit i uppsatsen anses det dock att det stora genombrottet för IoT ännu inte sett dagens ljus. Det förutspås att antalet IoT-objekt kommer att tredubblas på bara tio år för att till år 2030 uppgå till 29 biljoner enheter världen över. Med tanke på de stora möjligheter som tekniken medför i kombination med ökad kunskap, utbrett nätverk och billigare beståndsdelar har vi med all säkerhet inte sett ens en bråkdel av vad IoT i framtiden kan komma att användas till.

IoT medför redan idag stora fördelar för den enskilde som innebär en effektiv, bekväm och resurssparande tillvaro. Tekniken innebär dock även stora dataskyddsproblem och integritetsrisker när alltmer personlig data, genom bland annat IoT-objekt, hamnar i omlopp utanför den enskildes kontroll. Det gör att den kan spridas och användas för ändamål bortom den enskildes vilja samt läggas till i ett större pussel som utgör den enskildes privatliv. Bland annat möjliggör tekniken en kartläggning av den enskildes vanor, lokalisering, känslor, preferenser, hälsotillstånd med mera. I EKMR framgår dock den enskildes rätt till skydd för privatliv som ska skydda mot ingripande i den enskildes personliga sfär. Rätt till respekt för privatliv samt skydd av personuppgifter framgår även i EU-stadgan. Det är alltså av största vikt att dessa mänskliga rättigheter respekteras och värnas om.

Som förstås i delavsnitt 3.3.1 om vad som utgör personuppgifter enligt dataskyddsförordningen är det en stor mängd information som behandlas genom IoT-objekt som räknas in under begreppet. Som framgått definieras personuppgifter brett som ”varje upplysning som avser en identifierad eller identifierbar fysisk person […]”. Det kan vara allt från information om en persons namn, lokaliseringsuppgift och puls till röst, åsikter och värderingar. Vidare räcker det med att en person är indirekt identifierbar för att en uppgift ska räknas som en personuppgift. För att en person ska vara indirekt identifierbar ska informationen göra det *möjligt* att identifiera personen. Som tidigare framgått krävs det alltså inte att den personuppgiftsansvarige har tillgång till alla uppgifter som gör en identifiering möjlig för att det ska räknas som en personuppgift. Vidare räknas även pseudonymiserade uppgifter som personuppgifter, så länge en person kan identifieras genom kompletterande information. Även uppgifter som anonymiserats innan behandling kan be-

höva betraktas som personuppgifter enligt artikel 29-gruppen, eftersom det genom den teknik som IoT innefattar finns risk för att anonymiserade uppgifter kan återidentifieras, se delavsnitt 3.3.1. Med hänsyn till vad som framkommit i avsnitt 2.4 om vad för data som samlas in genom IoT-objekt står det klart att sådan insamlad data till mycket stor del är att betrakta som personuppgifter. Särskilt då komplicerade dataprocesser som sensor fusion och big data-analyser kan göra att till synes opersonlig information kan bidra till att en person direkt eller indirekt kan identifieras. En stor del av den information som samlas in genom IoT-objekt faller alltså utan tvekan in under dataskyddsförordningens tillämpningsområde.

IoT-tekniken möjliggör alltså insamling av enorma mängder data om enskilda personer och deras privatliv. Inte bara framgår det att enskilda inte alltid vet vilken information de delar med sig av. Dels genom att alla inte ens är medvetna om ifall de har något IoT-objekt i sin närhet som samlar in data om dem, dels genom att IoT-objekten kan samla in mer information än vad som är direkt uppenbart för den enskilde. Även i de fall konsumenten är medveten om datainsamlingen och hur den hanteras möjliggör IoT-tekniken att det, genom sensor fusion och big data-analyser, kan skapas mycket detaljerade profiler om användaren samt att informationen kan användas för helt andra ändamål än konsumenten haft anledning att förutse. Konsumenten kan även vara omedveten om med vilka insamlad data delas, eller ens *att* den delas. Detta visar på den stora risken för enskildas integritet när det kommer till IoT-objekt och det faktum att det kan vara nästintill omöjligt för den enskilde att bedöma värdet av den information denne delar med sig av. Det är således angeläget att det föreligger ett regelverk som kan möta dessa problem och låta den enskilde behålla kontrollen över sin personliga data och hur den används.

Som framgått är just det ett av syftena med dataskyddsförordningen – att låta den enskilde ha kontroll över sin personliga data genom att skydda deras grundläggande rättigheter och friheter, särskilt personuppgifter. Som framkom i bakgrundsavsnittet 1.1 är det av stor vikt att undersöka hur väl dataskyddsförordningen dock är lämpad för utvecklad teknik som IoT. Dels på grund av noteringen att IoT redan idag är en del av många personers vardag men som kommer få ännu större betydelse i framtiden, dels på grund av att det är dataskyddsförordningen som huvudsakligen är tänkt att reglera detta område. För att undersökningen ska utföras inom en rimlig ram undersöks dock endast den lagliga grunden samtycke, eftersom denna är en av grundpelarna i dataskyddsförordningen. Dessutom är just samtycke en av få lagliga grunder som i normalfallet blir tillämpliga för att kunna behandla enskildas personuppgifter när det kommer till deras användning av IoT. I många fall bör erhållande av den enskildes samtycke för övrigt vara det enda tillvägagångssätt för personuppgiftsansvariga att behandla IoT-konsumentens personuppgifter, eller, rättare sagt, den enskildes uttryckliga samtycke, se avsnitt 3.6 och 4.3. Detta återkommer jag till senare.

5.2 Den enskildes givande av samtycke

Som framkommit innehåller dataskyddsförordningen inget formkrav för på vilket sätt samtycke ska ges. Den personuppgiftsansvarige kan alltså själv utforma sätt för hur konsumenten ska ge samtycke. I och med den stora variation av kommunikationssätt när det kommer till IoT, som framkom i avsnitt 2.3, ges den personuppgiftsansvarige stora möjligheter att utforma ett tillvägagångssätt för givande av samtycke som passar just det specifika IoT-företaget och det specifika IoT-objektet. Som dataskyddsförordningen dock uppställer krävs det att samtycket utgör en otvetydig viljeyttring, antingen genom ett uttalande eller en entydig bekräftande handling. Det måste alltså vara utom tvivel att den enskilde haft för avsikt att samtycka till just den eller de specifikt angivna ändamål för behandling av den enskildes personuppgifter. Som EDPB framför skulle en entydig bekräftande handling exempelvis kunna vara att den enskilde viftar framför en smartkamera eller vrider en mobil medurs eller i en åtta. Båda dessa tillvägagångssätt kan förmodligen många gånger enkelt översättas till en IoT-kontext. I och med de många kommunikationssätt som tekniken möjliggör bör samtycke även kunna ges genom exempelvis tal, om IoT-objektet är utrustat med mikrofon, eller genom att trycka på en knapp på en skärm som tydligt markerar att det innebär ett samtycke. Det skulle alltså förutsätta att IoT-objektet de facto har en skärm. Även att samtycka via en app som är kopplad till IoT-objektet bör kunna utgöra en otvetydig viljeyttring. Sätt att ge samtycke på i IoT-sammanhang bör i de flesta fall således inte innebära något problem, så länge sättet inte kan rymma några tvivel om att den enskildes avsikt varit att samtycka till den specifika personuppgiftsbehandlingen. Den personuppgiftsansvarige måste dock säkerställa att den enskilde har möjlighet att återkalla sitt samtycke lika lätt som det är att ge det. Den personuppgiftsansvarige måste slutligen även kunna bevisa att det är just ett samtycke som har erhållits samt att samtycket är lämnat just av den registrerade och inte någon annan.

5.3 En uppenbar informationsproblematik

Ett uppenbart problem som dock uppstår kopplat till IoT är mängden information som måste tillhandahållas konsumenten för att denne ska kunna anses ge ett informerat, och därmed giltigt, samtycke. Som framkommit måste den registrerade informeras bland annat om den personuppgiftsansvariges identitet, syftet med varje personuppgiftsbehandling det begärs samtycke för, vilken typ av data som kommer behandlas, den registrerades rätt att återkalla sitt samtycke, med mera. Som EDPB dock skriver kan det vara tvunget att den registrerade måste erhållas mer information för att denne genuint ska kunna förstå hur personuppgifterna kommer att behandlas. Även EU-domstolen har uttalat att det krävs att den enskilde har möjlighet att avgöra följderna av ett samtycke. Det innebär att även IoT-objektens komplicerade teknik, med dess algoritmer och komplexa processer, måste förklaras i tillräcklig mån för att den enskilde ska kunna göra en egen utvärdering av

behandlingen och vad konsekvenserna av ett samtycke faktiskt kommer att bli.

Som framkommit i uppsatsen är IoT-tekniken så pass komplex att det innebär stora svårigheter att beskriva dessa dataprocesser på ett lättbegripligt sätt. För att ändå göra ett genuint försök att förklara dessa processer på ett sätt som är lättbegripligt för gemene man krävs det dock troligen långa informationstexter för att förklara hur tekniken fungerar och vad den kan åstadkomma. Det motverkar dock i sig kravet att den enskilde ska vara informerad, eftersom EU-befolkningen uppger att den största anledningen till att de väljer att inte läsa information relaterat till deras personliga integritet är att informationen är för lång. Denna respons var dessutom alltså enbart relaterad till sådan information som krävs för att förstå hur enskildas personuppgifter behandlas på internet, utan närvaron av komplexa processer som exempelvis sensor fusion. Dessutom verkar befolkningen bli mindre och mindre benägen att läsa integritetsrelaterad information, troligen på grund av att folket överöses med sådan information nästintill dagligen. Det gör att det uppstår vad man skulle kunna kalla en informationströtthet och är inte något dataskyddsförordningen bör främja eftersom det motverkar hela syftet med förordningen.

Som EDPB dock framhåller skulle informationen kunna delges i olika etapper för att underlätta för konsumentens intagande av informationen. Det skulle kunna medföra att den enskilde inte blir överväldigad av att överösas med all information på en gång. Frågan är dock om det är möjligt att dela upp all den information som måste erhållas i tillräcklig mån för att den enskilde inte ska bli lamslagen av mängden information. All nödvändig information måste ju onekligen erhållas i ett mycket tidigt skede, det vill säga innan den enskilde samtycker till personuppgiftsbehandlingen och IoT-objektet ens kan börja ha ett värde.

Med tanke på hur komplex IoT-tekniken kan vara, samt vad man får anta är nivån av gemene mans förståelse av sådan teknik, innebär det vidare att information om tekniken kommer vara svårförstådd för majoriteten. Även det motverkar dataskyddsförordningens syfte, eftersom EU-befolkningen uppger att även det faktum att informationen är oklar och svår att förstå är en annan tungt vägande orsak till att de väljer att inte läsa integritetsrelaterad information.

Om den enskilde inte erhålls sådan information som redogjorts för, eller om den är för lång och svårförstådd som gör att den enskilde väljer att inte läsa den, hindras den enskilde att inta en egen kritisk ståndpunkt. Det medför att den enskilde inte kan utöva självständig och full kontroll över sina personuppgifter, vilket är ett av dataskyddsförordningens tyngst vägande syften. Om det i praktiken är i princip omöjligt att tillhandahålla den enskilde all den information som krävs för att ett samtycke ska anses vara informerat

innebär det även att IoT-företagen i praktiken utsätts för stora utmaningar att ens ha möjlighet att följa lagstiftningen. Detta gäller särskilt då dataskyddsförordningen samtidigt ställer krav på att all information ska vara klar, tydlig och lättbegriplig.

Att IoT-företaget som personuppgiftsansvarig blir skyldigt att i så pass stor utsträckning förklara de dataprocesser som personuppgifterna behandlas genom skulle dessutom i princip kunna innebära att företaget blir tvunget att avslöja affärshemligheter och immateriella rättigheter, såsom patent. Det skulle kunna dämpa det kommersiella intresset och resultera i att den tekniska utvecklingen bromsas. Dessutom framgår det i skäl 63 i dataskyddsförordningen att den registrerades rätt till information inte bör inverka menligt på andras rättigheter, exempelvis affärshemligheter. Utifrån textens utformning står det dock klart att åtminstone viss inverkan är tillåten. Vad som i detta sammanhang utgör ”menlig” inverkan får anses vara oklart.

Informationsproblematiken blir vidare särskilt en utmaning då IoT-objekt ofta är små och saknar en skärm, eller endast har en liten sådan. Det innebär utmaningar att på ett rimligt sätt tillhandahålla konsumenten den information som krävs för att den ska kunna avge ett specifikt, informerat och giltigt samtycke. I stället måste sådan information tillhandahållas på annat håll, exempelvis på ett informationsblad som medföljer i samma förpackning som IoT-objektet, på IoT-företagets hemsida eller i en tillhörande mobilapp. Att läsa långa texter på en liten mobilskärm kan nog dock inte sägas vara optimalt i förhållande till syftet att underlätta för konsumentens inläsning och förståelse. Vi är nog alla av åsikten att det krävs en viss bokstavsstorlek och läsyta för att inläsningen av en ansenlig mängd information inte ska bli för utmanande. Att hänvisa till företagets hemsida är nog likaledes inte heller optimalt då det kräver att den enskilde utför ytterligare en handling för att kunna ta till sig informationen. En information som den redan från början sannolikt inte är särskilt sugen på att läsa.

5.4 Frivilligt samtycke?

Som framkom tidigare i delavsnitt 4.2.2.3 kan det ifrågasättas huruvida den registrerade faktiskt kan anses lämna ett helt genuint och frivilligt, och därmed giltigt, samtycke till personuppgiftsbehandling när det gäller IoT-objekt. Detta då IoT-objektet förlorar sitt funktionella värde om det inte kan samla in den data som behövs för att det ska fungera ändamålsenligt. Samtycket blir med andra ord ett måste för att IoT-objektet ens ska fungera. Det har ju dock varit frivilligt för den enskilde om denne ska införskaffa IoT-objektet eller inte, och konsumenten bör vid införskaffandet ha varit medveten om att objektet implicit eller explicit samlar in data. Däremot kan det vara så att den enskilde vid införskaffandet inte insåg omfattningen av den information som krävs eller på vilket sätt informationen behandlas. Dessutom kan det med vissa objekt vara svårt att förstå att det ens är ett datainsamlande IoT-objekt, vilket framkommit tidigare i avsnitt 2.3. I de fallen får

det sägas att den enskilde inte tidigare varit medveten om datainsamlingen och därmed inte tidigare haft ett val huruvida personen samtycker till behandlingen av sina personuppgifter eller inte. Frågan huruvida den enskildes samtycke i IoT-sammanhang kan anses vara frivilligt är alltså en rimlig sådan.

Om den enskilde i praktiken inte kan lämna ett helt frivilligt samtycke i IoT-sammanhang innebär det inte bara att personuppgiftsbehandlingen blir olaglig. Det innebär även att IoT-företagen som personuppgiftsansvariga inte har någon reell möjlighet att följa lagen. Detta särskilt med tanke på, som tidigare framkommit, att uttryckligt samtycke i många fall bör anses vara den enda grund som kan göra en personuppgiftsbehandling tillåten. Om den enskilde inte kan lämna ett genuint frivilligt samtycke innebär det även att den enskilde inte har full kontroll över sin personliga information. Som kommissionen framfört leder en minskad kontroll över enskildas egna personuppgifter till att enskilda får minskat förtroende för den digitala marknaden. Det skulle resultera i ett bakslag för IoT-marknaden, vilket i sin tur skulle innebära att den tekniska utvecklingen hämmas.

5.5 Förhållandet till dataskyddsförordningens grundläggande principer

Vidare uppstår utmaningar med IoT-tekniken särskilt i förhållande till några av de grundläggande principerna som genomsyrar hela dataskyddsförordningen. Som framkom ovan innebär det stora svårigheter att på ett tydligt och enkelt sätt informera om hur komplicerade dataprocesser, som sensor fusion och big data-analyser, fungerar samt hur den enskildes personuppgifter kommer hanteras genom dem. Det utgör en utmaning i förhållande till öppenhetsprincipen som stipulerar att all information och kommunikation ska vara klar, tydlig och lättbegriplig. Även faktumet att många IoT-objekt samlar in en ansenlig mängd information från sina sensorer kan innebära svårigheter för den personuppgiftsansvarige att förutse vilken data som kommer samlas in. Det innebär i sin tur svårigheter att på ett klart, tydligt och lättbegripligt sätt informera den enskilde om hur och vilken data som kommer behandlas. Mängden information och faktumet att IoT-objekt ofta är utformade att märkas så lite som möjligt innebär även att den enskilde inte alltid är medveten om vilken data som samlas in och hur den används. Det strider mot principen om korrekthet (fairness) som stipulerar att den registrerade alltid ska vara fullt medveten om vilken information som samlas in och hur den behandlas.

Att stora mängder information samlas in och som genom komplicerade dataprocesser möjliggör att extensiva slutsatser kan dras innebär vidare risk för brott mot principen om ändamålsbegränsning. Detta då det i sådana fall föreligger en stor risk för att personuppgifter samlas in och behandlas för andra och oförenliga ändamål i förhållande till de ursprungligt angivna än-

damålen. Det kan då förekomma så kallat ändamålsglidning. Att den personuppgiftsansvarige på förhand måste ange specifika ändamål för behandlingen får däremot anses hämma den tekniska utvecklingen. Detta då den personuppgiftsansvarige hindras att nyttja de många oförutsedda möjligheter som skapas genom tekniken. Principen om uppgiftsminimering utmanar vidare benägenheten till datamaximering, det vill säga tendensen att med IoT-objekt samla in uppgifter som i nuläget inte är aktuella men som kan vara användbara i framtiden. Av samma anledning kan det även sägas att principen om uppgiftsminimering hämmar den tekniska utvecklingen. Oförutsedda upptäckter som skulle kunna ha en positiv inverkan på utvecklingen förhindras därmed. En avvägning mellan enskildas integritetsskydd och den tekniska utvecklingen måste dock bevisligen göras. Frågan är dock om inte en specifik reglering, som är utarbetad med särskild hänsyn till denna typ av teknik och dess förutsättningar, på ett bättre sätt hade kunnat skapa en mer precis och balanserad reglering som både skulle kunna möta behovet av integritetsskydd och teknisk utveckling.

Vidare måste den personuppgiftsansvarige se till att verifiera att användaren av IoT-objektet är den registrerade och inte någon annan för att inte information om olika användare ska kunna registreras under en användares profil. Det skulle annars innebära att felaktiga uppgifter i relation till den registrerade behandlas, vilket skulle strida mot principen om korrekthet (accuracy) som kräver att alla uppgifter är korrekta. Även noteringen att IoT-objekt genom profilering kan skapa profiler med felaktiga förutsägelser innebär problem i förhållande till principen.

5.6 Uttryckligt samtycke

Som kort nämndes ovan bör det i många fall krävas att IoT-företaget erhåller konsumentens uttryckliga samtycke för att behandling av personens personuppgifter ska vara tillåten. Detta då det med tanke på den extensiva kartläggning av enskildas privatliv som möjliggörs med hjälp av IoT-tekniken inte bör vara en orimlig slutsats att en stor del av den data som samlas in bör betraktas som känsliga uppgifter. Som framkommit tidigare i avsnitt 4.4 skulle det till exempel vara möjligt att genom information om en persons matvaruinköp i kombination med data om livsmedlens kvalitet och energiinnehåll dra slutsatser om personens hälsotillstånd. Som framkommit bör alltså den registrerades uttryckliga samtycke i många fall vara den enda grunden genom vilken IoT-företaget kan behandla sådan information, se diskussion i avsnitt 4.3. Vidare kan det vara så att den personuppgiftsansvarige inte alltid på förhand vet vilka slutsatser som kommer frambringas då information från ett IoT-objekt samkörs med annan information. Den personuppgiftsansvarige kan alltså i sådant fall inte vara säker på att de personuppgifter som kommer att behandlas inte är känsliga sådana. Den kan inte heller vara säker på, då personuppgifterna behandlas genom enbart automatiserat beslutsfattande, att beslutet inte har sådana rättsliga följder för den enskilde, eller på liknande sätt i betydande grad påverkar denne, som fram-

går i avsnitt 4.4. Med tanke på den stora sannolikheten att känsliga uppgifter frambringas, eller att automatiska beslut tas som får betydande följder, kan det vara lämpligt att IoT-företaget redan från början erhåller ett uttryckligt samtycke från den registrerade. Detta för att undvika att oavsiktligen bryta mot lagen. Vad för praktisk skillnad det däremot är mellan ett vanligt samtycke och ett uttryckligt sådant får dock anses vara oklart, se vidare diskussion i avsnitt 4.3.

5.7 Dataskyddsförordningens mål om att vara teknikneutral

I relation till dataskyddsförordningens mål att vara en teknikneutral lagstiftning kan det med hänvisning till ovan framkomna analyser och slutsatser ifrågasättas om det är ett mål som faktiskt uppfylls. Som framkommit innebär den utvecklade teknik som IoT utgör en betydande distinktion från annan typ av personuppgiftsbehandling som dataskyddsförordningen också omfattar, såsom hantering av föreningsmedlemmars personuppgifter eller personers användning av webbplatser på internet. Med IoT:s särskiljande och komplexa teknik skapas helt andra förutsättningar och problem. Relaterat till ovan beskrivna problematik med dataskyddsförordningens reglering i förhållande till IoT kan det konstateras att förordningen inte lyckas reglera denna typ av teknik på ett helt ändamålsenligt sätt. Det får även sägas att förordningen missgynnar den. Detta gäller särskilt i relation till alla de sätt genom vilka dataskyddsförordningen hämmar den tekniska utvecklingen av tekniken samt skapar stora svårigheter att ens ha möjlighet att följa den. Dataskyddsförordningen uppfyller därmed inte sitt mål om att vara teknikneutral. Från ett annat perspektiv kan det även konstateras att förordningen, på grund av sitt mål att vara teknikneutral, missar chansen att särskilt reglera denna typ av teknik och på allvar bidra till en modernisering av EU:s dataskyddslagstiftning.

5.8 Samtycke som lämplig grund för behandling av personuppgifter

Slutligen kan det ifrågasättas om samtycke över huvud taget är en lämplig grund för tillåtelse av personuppgiftsbehandling när det kommer till IoT. Detta eftersom det, i och med IoT-teknikens komplexa och möjlighetsrika natur, finns stor risk att den enskildes personuppgifter behandlas på sätt eller för ändamål som denne inte är medveten om. Detsamma gäller med tanke på att det även förekommer att uppgifter ändrar karaktär. Från att utgöra till synes opersonliga uppgifter till att utgöra personuppgifter, samt från att utgöra vanliga personuppgifter till att räknas som känsliga sådana. Då detta kan ske utan att den enskilde är medveten om det kan det vara i princip omöjligt för den enskilde att bedöma värdet av sin personliga information. Genom dessa situationer förlorar således den enskildes rätt till självbestämmande genom samtycke sin betydelse. I stället blir den enskildes upplevda

kontroll endast en illusorisk sådan, och i stället för att stärka den enskildes ställning resulterar det i själva verket i en försvagning.

6 Slutsats

Sammanfattningsvis får det sägas att dataskyddsförordningen utgör ett skapligt försök att skydda enskilda personers integritet. I förhållande till IoT uppstår dock en problematik som gör att förordningens reglering kan ifrågasättas. Inte minst då IoT-tekniken innebär stora utmaningar för enskilda att ta vara på sina rättigheter och behålla en verklig kontroll över sin personliga information. Detta är något som dataskyddsförordningen inte tycks kunna reglera med ett rimligt utfall. På grund av de stora svårigheterna för enskilda att behålla en verklig kontroll över sin personliga information kan det dessutom ifrågasättas om samtycke över huvud taget är en lämplig grund för tillåtelse av personuppgiftsbehandling.

Vidare saknar IoT-företagen många gånger en reell möjlighet att uppfylla de krav som ställs för att kunna anses erhålla ett giltigt samtycke. Detta gäller särskilt den informationsproblematik som uppstår i förhållande till IoT och dess komplexa teknik samtidigt som förordningen kräver att all information ska vara klar, tydlig och lättbegriplig. Även faktumet att det kan ifrågasättas om det ens är möjligt för den enskilde att lämna ett helt genuint och frivilligt samtycke i IoT-sammanhang kan innebära stora svårigheter för IoT-företagen att följa lagen. Detta då samtycket i sådant fall inte skulle vara giltigt och andra grunder för personuppgiftsbehandling många gånger saknas. Trots att dataskyddsförordningen avser att vara modern och anpassad för ny teknik uppstår alltså problem för IoT-företagen att erhålla giltigt samtycke och därmed kunna erbjuda några produkter av värde. Eftersom bestämmelserna inte är praktiskt möjliga att följa brister lagstiftningen dessutom i att skydda enskildas personliga integritet.

Därutöver får regleringen i många fall anses hämma den tekniska utvecklingen. Detta gäller bland annat kopplat till att det leder till minskat förtroende för IoT-marknaden om den innebär att enskilda inte kan ha verklig kontroll över sin personliga information, samt att IoT-företagen i princip kan bli tvungna att avslöja affärshemligheter på grund av informationskraven. Dessutom innebär dataskyddsförordningens nuvarande reglering med ändamålsbegränsning och uppgiftsminimering att alla oförutsedda upptäckter som skulle kunna ha en positiv inverkan på utvecklingen förhindras.

Slutsatsen är således att dataskyddsförordningen, särskilt med beaktande av den lagliga grunden samtycke, inte är tillräckligt anpassad i förhållande till IoT för att funktionera ändamålsenligt. Frågan uppkommer om det som krävs inte är en särskild lagstiftning som kan ta specifik hänsyn till IoT och liknande teknikers särskiljande och komplexa natur. En sådan skulle mer precist och på ett bättre sätt kunna reglera teknikens utmaningar och förutsättningar. En sådan reglering skulle enligt min mening krävas för att EU ska kunna skydda sina medborgares personliga integritet och på allvar uppnå sitt mål om att vara världsledande i det datadrivna samhället.

Källförteckning

Offentligt tryck

EU-rättsligt offentligt tryck

Europeiska kommissionen

Kommissionens meddelande ”Mot ett nytt regelverk för infrastruktur för elektronisk kommunikation och tillhörande tjänster”, KOM(1999) 539 slutlig

Kommissionens meddelande ”Sakernas Internet – En handlingsplan för Europa”, KOM(2009) 278 slutlig

Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), KOM(2012) 11 slutlig

Europeiska kommissionen, Special Eurobarometer 487a: The General Data Protection Regulation, publicerad juni 2019

Kommissionens meddelande ”Dataskydd som en pelare för medborgarnas egenmakt och EU:s strategi för den digitala övergången – tillämpning av den allmänna dataskyddsförordningen under två års tid”, KOM(2020) 264 slutlig

Europeiska dataskyddsstyrelsen

EDPB, ”Endorsement 1/2018”, Bryssel, 25 maj 2018

EDPB, ”Guidelines 05/2020 on consent under Regulation 2016/679”, version 1.1, antagen 4 maj 2020 (EDPB Guidelines 05/2020)

EDPB, ”Guidelines 01/2022 on data subject rights – Right of access”, version 2.0, antagen 23 mars 2023 (EDPB Guidelines 01/2022)

Europeiska datatillsynsmannen

EDPS, ”Formal comments on the draft Commission Implementing Regulation on interoperability requirements and non-discriminatory and transparent

procedures for access to metering and consumption data”, antagen 24 augusti 2022

Artikel 29-gruppen

WP 136, Article 29 Data Protection Working Party, ”Opinion 4/2007 on the concept of personal data”, antagen 20 juni 2007

WP 169, Article 29 Data Protection Working Party, ”Opinion 1/2010 on the concepts of ”controller” and ”processor””, antagen 16 februari 2010

WP 187, Article 29 Data Protection Working Party, ”Opinion 15/2011 on the definition of consent”, antagen 13 juli 2011

WP 202, Article 29 Data Protection Working Party, ”Opinion 02/2013 on apps on smart devices”, antagen 27 februari 2013

WP 203, Article 29 Data Protection Working Party, ”Opinion 03/2013 on purpose limitation”, antagen 2 april 2013

WP 223, Article 29 Data Protection Working Party, ”Opinion 8/2014 on the Recent Developments on the Internet of Things”, antagen 16 september 2014

WP 251, Article 29 Data Protection Working Party, ”Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, senast reviderad och antagen 6 februari 2018

WP 259, Article 29 Data Protection Working Party, ”Guidelines on consent under Regulation 2016/679”, senast reviderad och antagen 10 april 2018

WP 260, Article 29 Data Protection Working Party, ”Guidelines on transparency under Regulation 2016/679”, senast reviderad och antagen 29 november 2017

Svenskt offentligt tryck

Utredningsbetänkanden och propositioner

SOU 2002:18 Personlig integritet i arbetslivet

SOU 2009:44 Integritetsskydd i arbetslivet

Prop. 2017/18:105 Ny dataskyddslag

Litteratur

Brill, Julie, ”The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control”, *Fordham Law Review*, vol. 83, issue 1, 2014, s. 205-217

Bugeja, Joseph, *Smart Connected Homes: Concepts, Risks, and Challenges*, Studies in Computer Science No 7, Malmö University, Faculty of Technology and Society, 2018

Bugeja, Joseph, Jacobsson, Andreas & Davidsson, Paul, “On Privacy and Security Challenges in Smart Connected Homes”, i *2016 European Intelligence and Security Informatics Conference (EISIC)*, Joel Brynielsson & Fredrik Johansson (red.), Uppsala, Sverige, 17-19 augusti 2016, s. 172-175

Bugeja, Joseph, Jacobsson, Andreas & Davidsson, Paul, ”An Empirical Analysis of Smart Connected Home Data”, i *Internet of Things – ICIOT 2018*, Dimitrios Georgakopoulos & Liang-Jie Zhang (red.), Seattle, WA, USA, 25-30 juni 2018, s. 134-149

Datainspektionen (f.d. Integritetsskyddsmyndigheten), ”Personuppgifter i genforskning – uppföljning av förhandskontroller”, 2002:4

Elvy, Stacy-Ann, ”Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond”, *Hofstra Law Review*, vol. 44, issue 3, 2016, s. 839-932

Frydlinger, David, m.fl, *GDPR: juridik, organisation och säkerhet enligt dataskyddsförordningen*, Första upplagan, Norstedts juridik, Stockholm, 2018

Greengard, Samuel, *The Internet of Things*, MIT Press, Cambridge, 2015

Hedtjärn Swaling, Vidar & Johansson, Jessica, *NCS3 Studie – IoT-relaterade risker och strategier*, Totalförsvarets forskningsinstitut (FOI), 2018, https://www.msb.se/RibData/Filer/pdf/28550.pdf

Hettne, Jörgen & Otken Eriksson, Ida (red.), *EU-rättslig metod: teori och genomslag i svensk rättstillämpning*, Andra upplagan, Norstedts juridik, Stockholm, 2011

Integritetsskyddsmyndigheten, ”Integritetsskyddsrapport 2020 – redovisning av utvecklingen på it-området när det gäller integritet och ny teknik”, 2021:1

Internetstiftelsen, *Svenskarna och internet 2019*, 2019, https://svenskarnaochinternet.se/app/uploads/2019/10/svenskarna-och-internet-2019-a4.pdf

Kleineman, Jan, ”Rättsdogmatisk metod”, i Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*, Andra upplagan, Studentlitteratur AB, 2018, s. 21-46

Krzysztofek, Mariusz, *GDPR: personal data protection in the European Union*, Kluwer Law International, Alphen aan den Rijn, 2021

Kuner, Christopher, m.fl. (red.), *The EU General Data Protection Regulation (GDPR): a commentary*, Första upplagan, Oxford University Press, Oxford, United Kingdom, 2020

Natarajan, Annamalai, m.fl., “Detecting Cocaine Use with Wearable Electrocardiogram Sensors”, I *UbiComp’13: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2013, Zürich, Schweiz, 8-12 september 2013, s. 123-132

Olsen, Lena, ”Rättsvetenskapliga perspektiv”, *SvJT*, 2004, s. 105-145

Peppet, Scott R., ”Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent”, *Texas Law Review*, vol. 93, issue 85, 2014, s. 85-179

Reed, Chris, ”Taking Sides on Technology Neutrality”, *SCRIPT-ed*, vol. 4, issue 3, 2007, s. 263-284

Reichel, Jane, ”EU-rättslig metod”, i Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*, Andra upplagan, Studentlitteratur AB, 2018, s. 109-142

Sundström, Tommy, *Internetguide #43 Internet of Things – En guide till sakernas internet*, Internetstiftelsen, 2016, https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

Svensson, Eva-Maria, ”De lege interpretata – om behovet av metodologisk reflektion”, *Juridisk Publikation*, 2014, s. 211-226

Thierer, Adam D., “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation”, *Rich. J. L. & Tech.*, vol. 21, issue 2, 2015

Wachter, Sandra, ”The GDPR and the Internet of Things: a three-step transparency model”, *Law, Innovation and Technology*, vol. 10, issue 2, 2018, s 266-294

Wendleby, Monika & Wetterberg, Dag, *Dataskyddsförordningen GDPR: förstå och tillämpa i praktiken*, Andra upplagan, Sanoma Utbildning, Stockholm, 2019

Öman, Sören, *Dataskyddsförordningen (GDPR) m.m.: en kommentar*, Andra upplagan, Norstedts juridik, Stockholm, 2021

Rättsfall

EU-domstolen

EU-domstolens dom av den 5 februari 1963, *Van Gend en Loos*, C-26/62, EU:C:1963:1

EU-domstolens dom av den 13 december 1989, *Grimaldi*, C-322/88, EU:C:1989:646

EU-domstolens dom av den 19 oktober 2016, *Breyer*, C-582/14, EU:C:2016:779

EU-domstolens dom av den 1 oktober 2019, *Planet49*, C-673/17, EU:C:2019:801

EU-domstolens dom av den 11 november 2020, *Orange România*, C-61/19, EU:C:2020:901

Svensk domstol

NJA 2005 s. 361

Övriga otryckta källor

EDPB. ”First Plenary of the European Data Protection Board”. Senast uppdaterad 25 maj 2018. Hämtad 24 april 2023. https://edpb.europa.eu/news/news/2018/first-plenary-european-data-protection-board_en

EDPB. ”Om oss”. u.å. Hämtad 24 april 2023. https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_sv

Europeiska kommissionen. “European data strategy – Making the EU a role model for a society empowered by data”. u.å. Hämtad 20 april 2023. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

Integritetsskyddsmyndigheten. ”Rättslig grund”. *Integritetsskyddsmyndigheten*. Senast uppdaterad 17 maj 2022. Hämtad 3 april, 2023. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/

Marchant, Natalie. ”What is the Internet of Things?”. *World Economic Forum*. Senast uppdaterad 31 mars 2021. Hämtad 16 februari 2023. https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/

Transforma Insights. “Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2023 (in billions)”. *Statista*. Senast uppdaterad 22 november 2022. Hämtad 16 februari 2023. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/