LUNDS UNIVERSITET
EKONOMI-
HÖGSKOLAN

Dataportabilitet och företagshemligheter

Balansgången mellan dataportabilitet och företagshemligheter

Alice Embe

INSTITUTIONEN FÖR HANDELSRÄTT

Affärsjuridisk kandidatuppsats

15 högskolepoäng

HARH13

VT 2024

Sammanfattning

Uppsatsen analyserar samspelet mellan rätten till dataportabilitet enligt EU:s dataskyddsförordning (GDPR) med skyddet för företagshemligheter enligt företagshemlighetsdirektivet. Syftet är att undersöka hur dess två regelverk påverkar varandra och hur en balans kan uppnås mellan individens rätt till sin data och företagens behov av att skydda känslig information. Uppsatsen klargör vad rätten till dataportabilitet innebär, definierar vad som räknas som företagshemligheter och analyserar hur dataportabiliteten kan begränsas av skyddet för företagshemligheter.

GDPR ger individer rätt att överföra sina personuppgifter från en tjänsteleverantör till en annan i ett strukturerat, allmänt använt och maskinläsbart format. Samtidigt skyddar företagshemlighetsdirektivet information med kommersiellt värde som hålls hemlig genom rimliga skyddsåtgärder.

Undersökningen påvisar en potentiell konflikt mellan GDPR och företagshemlighetsdirektivet, då företagshemligheter kan ingå i de data som individer har rätt att överföra enligt GDPR. Slutsatsen är att, även om rätten till dataportabiliteten är avgörande för individens kontroll över sina personuppgifter, måste denna rätt balanseras mot behovet av att skydda företagshemligheter för att säkerställa att ingen av dessa viktiga intressen åsidosätts. Denna konflikt har troligen bara inletts, och spänningarna mellan datainsamling och skyddet av personlig integritet kommer sannolikt att fortsätta vara en central fråga. Vilken som väger tyngst av dessa intressen blir förmodligen en tolkningsfråga, ofta präglad av politiska perspektiv och skiljelinjer.

Ämnesord: Dataportabilitet, dataskydd, företagshemligheter, företagshemlighetsdirektivet, GDPR, sekretess

Abstract

The thesis analyzes the interplay between the right to data portability under the EU General Data Protection Regulation (GDPR) and the protection of trade secrets under the Trade Secrets Directive. The aim is to examine how these two frameworks interact with each other and how a balance can be achieved between an individual's right to their data and the need for businesses to protect sensitive information. The thesis clarifies what the right to data portability entails, defines what constitutes trade secrets, and analyzes how data portability may be limited by the protection of trade secrets.

GDPR gives individuals the right to transfer their personal data from one service provider to another in a structured, commonly used, and machine-readable format. At the same time, the Trade Secrets Directive protects information of commercial value that is kept secret through reasonable protective measures.

The study highlights a potential conflict between GDPR and the Trade Secrets Directive, as trade secrets may be included in the data that individuals have the right to transfer under GDPR. The conclusion is that, although the right to data portability is crucial for individuals' control over their personal data, this right must be balanced against the need to protect trade secrets to ensure that neither of these important interests is compromised. This conflict has likely only just begun, and the tensions between data collection and the protection of personal privacy are likely to remain a central issue. Which of these interests will ultimately weigh the most will probably be a matter of interpretation, often shaped by political perspectives and dividing lines.

Keywords: Data portability, data protection, trade secrets, trade secrets directive, GDPR, confidentiality

Innehåll

Förkortningar

EDPB	Europeiska dataskyddsstyrelsen
EU	Europeiska unionen
FEUF	Fördraget om Europeiska unionens funktionssätt
GDPR	General Data Protection Regulation
IMY	Integritetsmyndigheten
LFH	Lag (2018:558) om företagshemligheter
Prop.	Proposition
SOU	Statens offentliga utredningar
f	Följande sida
ff.	Följande sidor

1 Inledning

1.1 Bakgrund

I dagens digitaliserade era har debatten om personlig integritet och dataskydd blivit allt viktigare. EU:s dataskyddsförordning, General Data Protection Regualtion (GDPR) som blev tillämplig i EU år 2018, markerade en viktig milstolpe i denna debatt. Förordningen syftar till att skydda fysiska personer med avseende på behandlingen av personuppgifter samt att möjliggöra det fria flödet av personuppgifter inom unionen.[1] En av nyheterna i GDPR är rätten till dataportabilitet, som återfinns i artikel 20. Denna rättighet ger individer möjlighet att överföra sina personuppgifter mellan olika tjänsteleverantörer, vilket stärker användarnas kontroll över sin data och främjar konkurrensen på marknaden.[2] Samtidigt innehåller EU-rätten bestämmelser om skydd för företagshemligheter, vilket regleras både genom företagshemlighetsdirektivet och motsvarande svensk lag. Företag investerar betydande resurser i att samla in och förädla data som utgör viktig del av deras affärsstrategier, såsom kundinformation och forskningsresultat.[3]

Här uppstår en konflikt: rätten till dataportabilitet kräver att företag möjliggör överföring av personuppgifter, vilket kan medföra risker att känslig affärsinformation inkluderas. Skäl 63 i GDPR betonar rätten för individer att få tillgång till sina personuppgifter och möjligheten att kontrollera behandlingen av dem, samtidigt som denna rätt inte får påverka andra rättigheter, såsom affärshemligheter. Å andra sidan betonar skäl 34 och 35 i företagshemlighetsdirektivet vikten av att skydda grundläggande rättigheter och friheter, inklusive skyddet av personuppgifter. Utmaningen ligger i att balansera individens rätt till dataportabilitet med företagens behov av att skydda sina företagshemligheter. Denna balansgång är avgörande för att skapa ett rättvist och effektivt digitalt landskap där både användarnas rättigheter och företagens intressen tillgodoses.

1.2 Syfte och frågeställningar

Uppsatsens syfte är att beskriva och analysera samspelet mellan rätten till dataportabilitet i EU:s dataskyddsförordning och skyddet för företagshemligheter enligt företagshemlighetsdirektivet.

För att uppnå detta syfte ska följande frågeställningar besvarats:

- Vad innebär rätten till dataportabilitet i EU:s dataskyddsförordning?

[1] David, Frydlinger; Tobias, Edvardsson; Caroline, Olstedt Carlström; Sandra, Beyer, *GDPR – Juridik, organisation och säkerhet enligt dataskyddsförordningen,* Stockholm: Norstedts Juridik AB, 2018, s. 29.
[2] WP 242 rev. 01 s. 3.
[3] Europeiska unionen (EU), *Trade Secrets,* 2024.

- Vad menas med företagshemligheter och vilket skydd får dessa enligt lagen om företagshemligheter?

- Hur begränsas rätten till dataportabilitet av skyddet för företagshemligheter?

Uppsatsen kommer att redogöra och analysera samspelet mellan rätten till dataportabilitet enligt GDPR och skyddet för företagshemligheter enligt företagshemlighetsdirektivet. Detta innebär att analysen begränsas till att utforska hur dessa två regelverk interagerar och de juridiska utmaningar som uppstår vid denna samverkan.

1.3 Metod och material

För att uppfylla uppsatsens syfte och besvara dess frågeställningar kommer både den rättsdogmatiska metoden och EU-rättsliga metoden att användas.

Uppsatsen använder rättsdogmatisk metod, vilket innebär att gällande rätt har fastställts genom en analys av rättskällor såsom lagstiftning, förarbeten, rättspraxis och doktrin.[4] Vidare strävar metoden efter att analysera och tolka den aktuella rätten inom ett specifikt rättsområde eller ämne, med fokus på att beskriva och systematisera rätten.[5] Rättskällornas auktoritet varierar beroende på deras natur: lagar och rättspraxis från högsta instanser har formell auktoritet, medans doktrinens auktoritet bygger på dess övertygande argument.[6] Förarbeten, särskilt uttalanden i propositioner, kan ibland ha formell auktoritet men behandlas ofta som en del av doktrinen, även om de generellt sett har en större betydelse än vanliga doktrinuttalanden. Kärnan i den rättsdogmatiska metoden är att hantera och tolka dessa rättskällor på ett systematiskt sätt med hänsyn till deras respektive auktoritet och påverkan på rättsområdet.[7]

EU-rättsligt material som ingår i studien har analyserats genom den EU-rättsliga metoden. Denna metod skiljer sig från svensk nationell rätt, särskilt genom att den ger mindre vikt åt förarbeten och istället betonar tolkning av lagar utifrån EU-domstolens praxis och de grundläggande fördragen. Inom EU-rätten bygger rättskällorna på en hierarkisk struktur som är avgörande för att förstå tillämpningen av lagstiftning och rättspraxis. Denna struktur kan delas in i tre huvudkategorier: primärrätt, sekundärrätt och icke-bindande normgivning. Primärrätten omfattar de grundläggande fördragen, såsom unionsfördraget, funktionsfördraget, rättighetsstadgan, samt de okodifierade allmänna rättsprinciperna.[8] Dessa bindande rättskällor tillämpas direkt i alla EU-medlemsländer utan att ytterligare implementering krävs.[9] Sekundärrätten omfattar främst lagstiftningstexter så som

[4] Jan Kleineman, Rättsdogmatisk metod. I *Juridisk metodlära.* Maria Nääv & Mauro Zamboni (red.), 21–46. 2 uppl. Lund: Studentlitteratur AB, 2018, s. 21.

[5] Åsa Gunnarsson, Eva-Maria Svensson, *Rättsdogmatik – som rättsvetenskapligt perspektiv och metod*, Lund: Studentlitteratur AB, 2023, s. 23.

[6] Ibid. 28–29.

[7] Ibid. 28.

[8] Ulf, Bernitz, Heuman, Lars, Leijonhufvud Madeleine, Seipel, Peter, Warnling-Nerep, Wiweka och Vogel, Hans-Heinrich, *Finna rätt: Juristens källmaterial och arbetsmetoder*, 16 u., Norstedts Juridik, Stockholm, 2023, s. 67.

[9] Jörgen, Hettne, & Ida, Otken Eriksson, *EU-rättslig metod. Teori och genomslag i svensk rättstillämpning.* 2 uppl. Stockholm: Norstedts Juridik AB. 2011. s. 40

förordningar, direktiv och beslut. I undersökningen behandlas två skyddsintressen som aktualiseras i både GDPR, som är en EU-förordning, och företagshemlighetsdirektivet, som är ett EU-direktiv. Dessa rättsakter utgör därmed en del av sekundärrätten inom EU och är underordnade primärrätten, vilket innebär att de alltid måste baseras på en rättsgrund i primärrätten. Enligt artikel 288 i FEUF har förordningar allmän giltighet och är direkt tillämpliga i alla EU-medlemsstater. Direktiven däremot ska implementeras av medlemsstaterna, som själva får bestämma form och tillvägagångssätt för genomförandet. Direktiv har en svagare genomslagskraft än förordningar. Även när medlemsstaterna införlivar direktiv i tid och på ett godtagbart sätt kan den närmare utformningen av den nationella lagstiftning som blir resultatet variera åtskilligt mellan länderna.[10] Inom unionsrätten finns fyra centrala tolkningsprinciper: språklig tolkning, systematisk tolkning, syftestolkning samt funktionell eller teologisk tolkning.[11] EU-rätten som behandlas i uppsatsen tolkas enligt dessa centrala principer.

Förordningar och direktiv inom EU inleds ofta med en ingress som innehåller beaktandesatser. Dessa satser, även om de inte har juridisk bindande kraft, spelar en avgörande roll som tolkningsverktyg för de efterföljande artiklarna.[12] I denna uppsats är tolkningen av beaktandesatser särskilt viktig, då de erbjuder insikter i de bakomliggande avsikterna och målen med lagstiftningen. GDPR och företagshemlighetsdirektivet hanterar komplexa och ibland motsägelsefulla skyddsintressen, och beaktandesatserna är centrala för att förstå och tolka dessa regelverk på ett nyanserat sätt.

I arbetet med att tolka dataskyddslagstiftningen, särskilt artikel 20 i GDPR, är vägledningar och riktlinjer från Europeiska dataskyddsstyrelsen (EDPB) av central betydelse. Även om EDPB:s riktlinjer inte är bindande rättsakter ger de viktiga insikter i hur regler bör tillämpas inom området. För att förstå och tolka EU-rättsakter används ofta icke-bindande dokument som utarbetats av olika EU-organ i samarbete med nationella aktörer.[13] Dessa dokument, såsom riktlinjer och vägledningar, syftar till att främja ett enhetligt och effektivt genomförande av lagstiftningen över hela EU.[14] EDPB har ersatt den tidigare Artikel 29-gruppen och fortsätter att spela en viktig roll genom att utfärda riktlinjer och rekommendationer som belyser tillämpningen av dataskyddsbestämmelserna.[15]

Utöver EDPB:s riktlinjer används även yttranden och vägledningar från Integritetsmyndigheten, Europeiska kommissionen samt relevanta juridiska artiklar och litteratur. Inspelade konferenser och beslut om sanktionsavgifter kopplade till GDPR är också viktiga källor. Eftersom det finns en brist på rättsfall och tydlig rättspraxis, är dessa källor avgörande för en djupare förståelse och tolkning av lagstiftningen.

[10] Bernitz, m.fl., 2023, s. 68 f.
[11] Bernitz, m.fl., 2023, s. 77 f.
[12] Bernitz, m.fl., 2023, s. 76 f.
[13] Bernitz, m.fl.,2023, s. 70.
[14] Hettne & Otken Eriksson, 2011, s. 47.
[15] Frydlinger m.fl., 2018, s. 82.

1.4 Disposition

Uppsatsen är uppdelad i fem kapitel som tillsammans syftar till att besvara de tre ovannämnda frågeställningarna (se avsnitt 1.2). Det första kapitlet är en introduktion som sedan följs av kapitel 2 som ger en bakgrund till GDPR och rätten till dataportabilitet. I kapitel 3 ges en redogörelse för skyddet av företagshemligheter enligt EU-rätten och svensk lag. Kapitel 4 behandlar samspelet mellan dataskydd och skyddet av företagshemligheter, och analyserar de potentiella konflikter som kan uppstå. I det femte och avslutande kapitlet genomförs en analys av det som har behandlats, med målet att besvara uppsatsens frågeställningar.

2 Rätten till portabilitet

2.1 Inledning

I detta kapitel kommer vi att utforska historien och utvecklingen av dataskyddsförordningen (GDPR), med särskild fokus på artikel 20 och den registrerades rätt till dataportabilitet. Vidare kommer vi även att gå igenom grundläggande begrepp som är relevanta för GDPR för att ge en klar och heltäckande förståelse av regelverket.

2.2 Dataskyddsförordningens framväxt

Före GDPR var dataskyddslagstiftningen i Sverige och andra länder inom EU betydligt mer begränsad. År 1973 antog Sverige den allra första nationella dataskyddslagstiftningen i världen, nämligen datalagen (1973:289). Datalagen innehöll inte detaljerade regler kring hur man skulle behandla personuppgifter, utan istället byggde lagen på kravet att man behövde tillstånd från Datainspektionen, nuvarande Integritetsskyddsmyndigheten för att få inrätta ett datoriserat personregister. Under 1970-talet följde flera västeuropeiska länder efter med liknande lagstiftningar, som också innehöll förbud mot att överföra personuppgifter utomlands.[16]

En betydande utveckling skedde genom Europarådets dataskyddskonvention från 1981, som etablerade dataskyddsprinciper för rådets medlemsstater.[17] Ett annat väsentligt steg i utvecklingen var *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*, även kallat dataskyddsdirektivet. Direktivet byggde vidare på de etablerade principerna i dataskyddskonventionen men preciserade och förstärkte dem för att hantera de nya kraven och utmaningar som uppkommit inom dataskyddet. Dataskyddsdirektivet införlivades i Sverige genom antagandet av personuppgiftslagen (1998:204) som trädde i kraft 1998. Lagen sågs som en ersättning och modernisering av datalagen från 1973.[18]

Med internets framväxt och globalisering blev det tydligt att dataskyddsdirektivets reglering inte längre räckte till.[19] Mot bakgrund av detta lämnade EU-kommissionen i början av 2012 fram ett förslag till ny dataskyddslagstiftning för att ersätta det föråldrande dataskyddsdirektivet från 1995. Förslaget till ny lag genomgick en lång process av förhandlingar och granskningar inom EU. I slutet av 2015 enades Europaparlamentet och rådet om en ny dataskyddsförordning och 2016 antogs *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*

[16] Sören, Öman, *Dataskyddsförordning (GDPR) m.m.- En kommentar,* 2 uppl. Stockholm: Norstedts Juridik AB, 2021, s. 17.
[17] Frydlinger m.fl., 2018, s. 23.
[18] Öman, 2021, s. 18.
[19] Öman, 2021, s. 19.

det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Dataskyddsförordnigen blev direkt tillämplig i alla medlemsstater den 25 maj 2018. Samtidigt upphävdes det tidigare dataskyddsdirektivet och personuppgiftslagen.[20]

GDPR är en omfattande lagstiftning som syftar till att harmonisera och stärka skyddet av personuppgifter för alla individer inom EU.[21] Målet med GDPR är att säkerställa en enhetlig och hög skyddsnivå för alla fysiska personer inom Europeiska unionen. GDPR strävar även efter att undanröja eventuella skillnader mellan medlemsstaterna som kan hindra det fria flödet av personuppgifter på den inre marknaden.[22] En viktig del av GDPR är rätten till dataportabilitet, som specificeras i artikel 20 och kommer att undersökas närmare i denna uppsats.

2.3 Grundläggande begrepp

Innan vi fördjupar oss ytterligare i rätten till dataportabilitet är det viktigt att definiera vad som menas med personuppgifter, personuppgiftsansvarig samt hur GDPR reglerar behandling av sådana uppgifter.

2.3.1 Personuppgifter

I artikel 4.1 i GDPR finner vi den juridiska definitionen av personuppgifter:

> ”varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikationer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.[23]

Personuppgifter innefattar alltså all form av information som på något sätt kan kopplas till en identifierad eller identifierbar individ som är i livet. Det kan omfatta en mängd olika data, såsom namn, adress, personnummer, telefonnummer, e-postadress och mycket mer. Även bild- och ljudupptagningar om en fysisk person räknas som personuppgifter. Uppgifter som har kodats eller krypterats men som med hjälp av kompletterande uppgifter går att koppla till en person ses fortfarande som personuppgifter.[24] Det förkommer även uppgifter som tilldelats ett särskilt starkt skydd enligt GDPR, detta på grund av att de anses som särskilt känsliga. Exempel på sådana känsliga uppgifter inkluderar bland annat etniskt ursprung, ras och sexuell läggning. För dessa typer av uppgifter gäller huvudregeln i artikel 9.1 som förbjuder deras behandling utan samtycke från den registrerade eller stöd av annat undantag som räknas upp i artikel 9.2.[25] I artikel 5 i GDPR fastställs de grundläggande principer som genomsyrar all behandling av personuppgifter. Dessa principer måste som utgångspunkt följas vid all behandling av personuppgifter, vilket innebär att behandlingen måste ha en rättslig grund och bland annat endast de personuppgifter

[20] Öman, 2021, s. 21.
[21] Skäl 3 i GDPR.
[22] Skäl 13 i GDPR.
[23] Artikel 4.1 i GDPR.
[24] Integritetsmyndigheten, ”*Ordlista - Personuppgifter”,* hämtad 2024-03-27, https://www.imy.se/ordlista/#P.
[25] Artikel 9.1 i GDPR.

som är nödvändiga för ändamålet med behandlingen.[26] Principerna innefattar laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, riktighet, lagringsminimering, integritet och konfidentialitet, samt ansvarsskyldighet.[27]

2.3.2 Personuppgiftsansvarig

En personuppgiftsansvarig är den enhet eller organisation som bestämmer ändamålen och medlen för behandlingen av personuppgifter. Detta kan vara en stiftelse, ett aktiebolag, en myndighet eller förening. Det är alltså varken chefen eller en enskild anställd som är personuppgiftsansvarig. Att vara personuppgiftsansvarig innebär att organisationen har det fulla ansvaret för att följa lagstiftningen och säkerställa att behandlingen av personuppgifter sker i enlighet med bestämmelserna i GDPR.[28]

En viktig del av detta ansvar är att säkerställa att all behandling av personuppgifter har en rättslig grund. Artikel 6 i GDPR fastställer de sex rättsliga grunderna för behandling av personuppgifter. Dessa grunder är samtycke, fullgörande av avtal, fullgörande av rättslig förpliktelse, skydd av intresse av grundläggande betydelse för en fysisk person, utförande av uppgift av allmänt intresse eller myndighetsutövning samt intresseavvägning.[29]

Ett företag är exempelvis normalt personuppgiftsansvarig för behandling av personuppgifter om sina anställda, kunder eller leverantörer. På liknande sätt är en myndighet personuppgiftsansvarig för behandling av uppgifter om personer som är involverade i ärenden hos myndigheten. Den som är personuppgiftsansvarig kan delegera den praktiska behandlingen av personuppgifter till andra men personuppgiftsansvaret kan aldrig överföras. Den personuppgiftsansvarige har ett övergripande ansvar att bedöma och hantera integritetsriskerna som är förknippade med behandlingen av personuppgifter. För att säkerställa och kunna bevisa att behandlingen följer GDPR måste lämpliga tekniska och organisatoriska åtgärder vidtas. Det kan innebära att man exempelvis antar en policy med relevanta strategier för dataskydd och ser till att dessa implementeras i hela organisationen. Certifieringar och uppförandekoder kan vara ett effektivt sätt att demonstrera att man lever upp till kraven i GDPR.[30]

2.3.3 Behandling

I GDPR definieras behandling som följande:

---

[26] Integritetsmyndigheten, ”*Grundläggande principer*”, hämtad 2024-04-01, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/ .

[27] Artikel 5 i GDPR.

[28] Integritetsmyndigheten, ”*Personuppgiftsansvariga och personuppgiftsbiträden”,* hämtad 2024-04-05, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

[29] Artikel 6 i GDPR.

[30] Integritetsmyndigheten, ”*Personuppgiftsansvariga och personuppgiftsbiträden”,* hämtad 2024-04-05, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

> ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring”. [31]

Behandlingen som omfattas av GDPR kan ske antingen helt eller delvis genom automatisk bearbetning eller manuell bearbetning av personuppgifter. I det senare fallet omfattas endast uppgifter som ingår i eller är avsedda att ingå i ett register. Automatisk bearbetning avser bearbetning som utförs med hjälp av datorer eller annan digital teknik.[32]

2.4 Rätten till dataportabilitet

Rätten till dataportabilitet är en central del av GDPR som syftar till att ge individer större kontroll över sina personuppgifter. Detta avsnitt kommer att utforska rätten till dataportabilitet, med särskild tonvikt på de rättigheter som tillkommer den registrerade samt de detaljerade bestämmelserna i artikel 20.

2.4.1 Den registrerades rättigheter

I GDPR hänvisas det till den registrerade som den person som kan identifieras genom de personuppgifter som behandlas. Den registrerade har i enlighet med GDPR tilldelats ett antal rättigheter som är avsedda att ge individen information om hur och när deras personuppgifter behandlas samt ge individen kontroll över sina uppgifter.[33] Dessa rättigheter specificeras i artiklarna 12–23. Bland dessa rättigheter finns rätten till dataportabilitet. Förutom denna rättighet inkluderar även GDPR rätten till information och tillgång, rättelse och radering, begränsning av behandling, invändning mot behandling samt särskilt skydd vid automatiserade beslut. Rätten till information för den registrerade om behandlingen av sina personuppgifter regleras i artiklarna 12–14 i GDPR.[34] Artikel 15 i GDPR innefattar den registrerades rätt till tillgång till sina personuppgifter med viss tillhörande information, exempelvis ändamålet med behandlingen.[35] I artikel 16 GDPR återfinns rätten till rättelse vilket innebär att den registrerade har rätt att, utan onödigt dröjsmål få felaktiga personuppgifter rättade.[36] Rätt till radering, även kallad rätten att bli bortglömd, enligt artikel 17 GDPR, innebär den personuppgiftsansvariges är skyldig att utan onödigt dröjsmål radera den registrerades personuppgifter om någon av de angivna omständigheterna i artikeln föreligger.[37] Rätten till begränsning av behandling återfinns i artikel 18 GDPR och innebär att den registrerade kan begära att behandlingen av dennes personuppgifter begränsas under vissa omständigheter.[38] Enligt artikel 21 GDPR har den registrerade rätt att göra invändningar mot vissa

[31] Artikel 4.2 i GDPR.
[32] Artikel 2.1 i GDPR.
[33] Integritetsmyndigheten,” *Den registrerades rättigheter”,* hämtad 2024-04-01, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/ .
[34] Skäl 58–62 i GDPR.
[35] Artikel 15.1, 15. 1a i GDPR.
[36] Artikel 16 i GDPR.
[37] Artikel 17 i GDPR.
[38] Artikel 18 i GDPR.

personuppgiftsbehandlingar.[39] I den sista artikeln av den registrerades rättigheter, i artikel 22 GDPR, återfinns den registrerades rätt att inte bli föremål för beslut som enbart grundas på automatiserad behandling, inklusive så kallad profilering.[40]

2.4.2 Rätten till dataportabilitet – en nyhet i dataskyddsförordningen

År 2000, när Europeiska unionens stadga om grundläggande rättigheter antogs, fick skyddet av personuppgifter en central plats genom artikel 8. Stadgan blev bindande den 1 december 2009 i och med Lissabonfördragets ikraftträdande, vilket ytterligare förstärkte skyddet genom att artikel 16 i Fördraget om Europeiska unionens funktionssätt fastställde individens rätt till skydd av sina personuppgifter.[41] I Sverige är rätten till skydd för den personliga integriteten även stadgad i grundlagen.[42] När GDPR blev tillämplig 2018 markerade det en ny era för dataskydd och personlig integritet. En av nyheterna i förordningen var införandet av rätten till dataportabilitet. Denna rättighet infördes för att stärka individens kontroll över sina personuppgifter och göra det lättare att överföra dem mellan olika tjänsteleverantörer. I praktiken innebär dataportabilitet att den registrerade har rätt att på begäran få ut eller flytta sina personuppgifter som rör honom eller henne från en tjänsteleverantör till en annan. Det är således individen som avgör vilka som har tillgång till uppgifterna och på vilket sätt de kan användas.[43] Genom portabilitetsrätten ges individen rätten att erhålla sina personuppgifter enligt sina egna villkor och önskemål.[44]

Artikel 20 i GDPR består av ett antal punkter och infördes för att förbättra individens kontroll över sina personuppgifter genom att göra det lättare att flytta, överföra och kopiera personuppgifter från en it-miljö till en annan.[45] Detta möjliggör för individer att effektivt flytta och hantera sina personuppgifter mellan olika organisationer och tjänsteleverantörer.[46] Artikeln stadgar att individer har rätt att begära att få ut sina personuppgifter som de tillhandahållit en personuppgiftsansvarig, i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade har även rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan hinder från den ursprungliga personuppgiftsansvarige, förutsatt att behandlingen grundar sig på samtycke eller ett avtal samt sker automatiserat. Rätten till dataportabilitet möjliggör även direktöverföring av uppgifter mellan ansvariga, när det är tekniskt möjligt. Dock får denna rättighet inte påverka andra rättigheter och friheter negativt och gäller inte för behandling som är nödvändig för att utföra uppgifter av allmänt intresse eller myndighetsutövning.[47]

I artikel 20.1 fastställs rätten att få ut sina personuppgifter från den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format. Det handlar om när registrerade har rätt att begära ut sina personuppgifter, som de själva har tillhandahållit den personuppgiftsansvarige, samt föreskriver hur den

[39] Artikel 21 i GDPR.
[40] Artikel 22 i GDPR.
[41] Öman, 2021, s. 20.
[42] Regeringsformen, 2 kap. 6§.
[43] Skäl 68 i GDPR.
[44] WP 242 rev.01, s 6.
[45] WP 242 rev. 01, s 4.
[46] Skäl 68 i GDPR.
[47] Skäl 68 i GDPR.

personuppgiftsansvarige ska lämna ut dessa uppgifter.[48] Dessa personuppgifter kan sedan lagras för personligt bruk, antingen på en privat enhet eller i ett privat moln. I denna kontext fungerar rätten till dataportabilitet som ett komplement till rätten till tillgång till personuppgifter i artikel 15 i GDPR. Vad som särskiljer dataportabiliteten är dess förmåga att göra det enkelt för de registrerade att själva hantera och återanvända sina personuppgifter.[49]

Artikel 20.2 betonar individens rätt att få sina personuppgifter överförda direkt från en personuppgiftsansvarig till en annan, om det är tekniskt genomförbart. Detta innebär att en användare enkelt kan byta tjänst eller plattform utan att förlora sina tidigare insamlade data.[50] Skäl 68 i GDPR uppmanar personuppgiftsansvariga att främja utvecklingen av kompatibla format för dataportabilitet. Trots detta är personuppgiftsansvariga inte juridiskt ålagda att införa eller upprätthålla sådana system. Detta innebär att det inte föreligger någon rättslig skyldighet för dem att tillhandahålla specifika mekanismer eller format för dataportabilitet. Dock förbjuder GDPR personuppgiftsansvariga från att skapa hinder för överföring av uppgifter. De får alltså inte agera på ett sätt som hindrar eller försvårar den registrerades rätt till dataportabilitet. Denna aspekt av dataportabilitet möjliggör inte bara att registrerade får tillgång till och kan använda sina uppgifter på nya sätt, de kan också flytta sina uppgifter till en annan tjänsteleverantör, inom samma eller annan sektor. Rätten till dataportabilitet förväntas även att främja innovation samt möjliggöra säker delning av personuppgifter mellan personuppgiftsansvariga. Dataportabiliteten möjliggör smidig överföring och återanvändning av användares personuppgifter mellan olika tjänster som de använder eller är intresserade av.[51]

I artikel 20.3 finner vi bestämmelsen som klargör att rätten till dataportabilitet inte är tillämplig i vissa fall, till exempel när det gäller sådan myndighetsutövning eller arbetsuppgift av allmänt intresse som avses i artikel 6.1 e. Dessutom påverkar inte denna rättighet den registrerades möjlighet att begära att deras data raderas från en organisation eller tjänst om så behövs enligt artikel 17 i förordningen.[52] Dataportabilitetsrätten är begränsad till fall där behandlingen av personuppgifter är automatiserad och baserad på den registrerades samtycke enligt artikel 6.1a eller 9.2a i förordningen, eller när behandlingen är nödvändig för att fullgöra ett avtal som den registrerade är part i enligt artikel 6.1b.[53]

Artikel 20.4 betonar att rätten till dataportabilitet inte får påverka andras rättigheter och friheter. Det innebär att även om en individ har rätt att överföra sina personuppgifter från en organisation till en annan, får inte denna rättighet kränka eller äventyra rättigheterna och friheterna hos andra registrerade eller den personuppgiftsansvarige.[54]

Utifrån de syften som rätten till dataportabilitet bygger på, framstår individens ökade kontroll som det mest centrala. Genom att ge individen möjlighet att själv få tillgång

[48] Öman, 2021, s. 374.
[49] WP 242 rev. 01, s
[50] Ibid.
[51] WP 242 rev. 01, s. 5.
[52] Öman, 2021, s. 377.
[53] Öman, 2021, s. 374.
[54] Öman, 2021, s. 373.

till uppgifterna i ett användbart format och fritt flytta dem mellan olika tjänsteleverantörer, strävar portabilitetsrätten efter att stärka denna kontroll.[55]

2.4.3 När den registrerade har rätt till dataportabilitet och hur den ska verkställas

Rätten till dataportabilitet är en relativt begränsad rättighet då en endast täcker personuppgifter som den registrerade själv har tillhandahållit den personuppgiftsansvarige. [56] Detta innebär att informationen som den registrerade har genererat genom sin egen aktivitet, till exempel kontouppgifter såsom e-postadress och användarnamn, men även sökhistorik och aktivitetsloggar omfattas av denna rättighet.[57] Det innebär att alla personuppgifter som den personuppgiftsansvarige har fått indirekt, och även all annan relevant data som inte klassificeras som personuppgifter, undantas från denna rättighet. Enligt artikel 20.1 i GDPR måste de uppgifter som omfattas av rätten till dataportabilitet uppfylla två huvudsakliga kriterier:

1. De måste vara personuppgifter som rör den registrerade.
2. De måste ha tillhandahållits av den registrerade till den personuppgiftsansvarige.

Det första villkoret innebär att endast personuppgifter ingår i tillämpningsområdet för dataportabiliteten. Det innebär att avidentifierade uppgifter eller uppgifter som inte rör den registrerade inte omfattas. Dock inkluderas pseudonymiserade uppgifter eftersom dessa kan kopplas till en registrerad. I många fall behandlar personuppgiftsansvarige information som involverar personuppgifter om flera registrerade. Trots att dessa uppgifter kan inkludera detaljer om tredje parter, bör den registrerade kunna få tillgång till dem genom en begäran om dataportabilitet, eftersom dessa uppgifter också rör den registrerade. Det är dock avgörande att den nya personuppgiftsansvarige som tar emot dessa uppgifter inte använder dem på ett sätt som skulle negativt påverka sådana tredje parters rättigheter och friheter.[58]

Det andra villkoret för dataportabilitet begränsar tillämpningsområdet till uppgifter som den registrerade aktivt har ”tillhandahållit”. Detta innefattar inte bara uppgifter som medvetet och aktivt lämnats av den registrerade, såsom kontouppgifter via nätformulär, utan enligt Artikel 29-gruppens bedömning också uppgifter som resultat av observationer av deras aktivitet. Detta inkluderar data som kan observeras från användarnas aktivitet, såsom rådata från exempelvis aktivitetsloggar. Däremot omfattar det inte uppgifter som skapats av den personuppgiftsansvarige genom att analysera data från användningen. Att även uppgifter som observerats från användning av tjänsten eller enheten kan klassificeras som ”tillhandahållna av den registrerade”, har kritiserats, men ska enligt riktlinjer från Artikel 29-arbetsgruppen som Europeiska dataskyddsstyrelsen ställt sig bakom omfattas av rätten till

[55] WP 242 rev. 01, s. 4.
[56] Frydlinger m.fl., 2018, s. 217.
[57] WP 242 rev. 01, s. 11.
[58] WP 242 rev. 01, s. 10.

dataportabilitet. Detta kan inkludera sökhistorik, trafikuppgifter, platsdata och andra insamlade rådata, till exempel hjärtfrekvens som mätts av en bärbar pulsmätare.[59]

En ytterligare begränsning är när man hänvisar till samtycke och avtal som grunder för behandlingen. Om den personuppgiftsansvarige utför behandlingen baserat på en intresseavvägning, finns det ingen skyldighet att lämna ut personuppgifterna. När den registrerade har rätt att få ut sina personuppgifter, ska dessa ges ut i ett strukturerat, allmänt användbart och maskinläsbart format. Detta bör tolkas som ett format som möjliggör för den registrerade att bearbeta uppgifterna vidare utan stora investeringar. Vidare ska den registrerade också ha rätt att överföra dem till en annan personuppgiftsansvarig, vilket innebär att det inte får finnas rättighetsmässiga begränsningar (se vidare nedan avsnitt 2.4.5).[60] Detta kan liknas vid ägande eller en mycket bred licens inom immaterialrätten, även om det inte finns ett heltäckande skydd för data som ett generellt begrepp. Den personuppgiftsansvarige som lämnar ut uppgifterna får inte begränsa den registrerades rättigheter att överföra informationen vidare.[61]

2.4.4 Skyldighet att överföra personuppgifter direkt till en annan personuppgiftsansvarig

Enligt artikel 20.1 i dataskyddsförordningen har registrerade rätt att överföra uppgifter till en annan personuppgiftsansvarig utan hinder från den som tillhandahållit uppgifterna. Hindren kan vara juridiska, tekniska eller ekonomiska och kan inkludera avgifter för datautlämning, bristande kompatibilitet i dataformat, orimliga förseningar eller försvårande åtgärder vid tillgång till data. Enligt artikel 20.2 är personuppgiftsansvariga skyldiga att överföra flyttbara uppgifter direkt till andra personuppgiftsansvariga, förutsatt att det är tekniskt möjligt. Överföring från en personuppgiftsansvarig till en annan kan ske när det finns möjlighet till säker kommunikation mellan två system och när det mottagandet systemet rent tekniskt kan ta emot de inkommande uppgifterna. Om tekniska hinder förhindrar direkt överföring bör den personuppgiftsansvariga informera de registrerade om dessa begränsningar. Underlåtenhet att göra det kan likställas med att ignorera den registrerades begäran enligt artikel 12.4 i förordningen.[62]

På en teknisk nivå bör personuppgiftsansvariga utforskat två kompletterande metoder för att tillhandahålla flyttbara uppgifter till registrerade eller andra personuppgiftsansvariga. Personuppgiftsansvariga kan utföra direkt överföring av antingen hela uppsättningen av flyttbara uppgifter eller utdrag från hela uppsättningen av uppgifter. De kan också använda automatiseringsverktyg för att extrahera relevanta uppgifter. Den andra metoden kan vara att föredra för personuppgiftsansvariga vid hantering av komplexa och omfattande datamängder, detta eftersom den möjliggör extrahering av relevanta delar av uppgifterna i samband med den registrerades begäran. Denna metod kan också bidra till att minimera risken genom att underlätta användningen av synkroniseringsmekanismer. Detta kan förbättra efterlevnaden för den nya personuppgiftsansvarige och samtidigt minska

[59] WP 242 rev. 01, s. 11.
[60] Frydlinger m.fl., 2018, s. 217.
[61] Frydlinger m.fl., 2018, s. 218.
[62] WP 242 rev. 01, s. 17.

integritetsriskerna för den ursprungliga personuppgiftsansvarige. För att tillhandahålla dessa flyttbara uppgifter kan olika metoder användas, såsom säker meddelandehantering och säkra webbaserade gränssnitt för webbportaler. Registrerade bör också ha möjlighet att använda lagringsplatser för personuppgifter eller andra betrodda tredje parter för att inneha och lagra data samt bevilja personuppgiftsansvariga åtkomst och behandlingstillstånd vid behov.[63]

2.4.5 Dataportabilitet får inte negativt påverka andras rättigheter

Artikel 20.4 i GDPR, som föreskriver att dataportabilitet inte får påverka andras rättigheter och intressen, innebär att det alltid är nödvändigt att göra en intresseavvägning. Vid denna avvägning är det viktigt att ta hänsyn till immateriella äganderätter och affärshemligheter. Även om dessa aspekter inte direkt relaterar till portabilitet kan de tolkas som inkluderande affärshemligheter och immateriell äganderätt, särskilt när det gäller upphovsrättsligt skydd för programvara. Även om sådana överväganden är viktiga bör de inte resultera i att man helt vägrar att tillhandahålla information om den registrerade. Samtidigt innebär rätten till dataportabilitet inte att man har rätt att missbruka informationen, vilket skulle kunna klassificeras som otillbörlig konkurrens eller intrång i immateriella rättigheter. Potentiella affärsrisker får dock inte användas som skäl för att helt och hållet neka en begäran om dataportabilitet. Personuppgiftsansvariga kan överföra personuppgifter som tillhandahållits av registrerade i ett format som inte avslöjar information som skyddas av affärshemligheter eller immateriella rättigheter.[64]

[63] WP 242 rev. 01, s. 18.

[64] WP 242 rev. 01, s. 14.

3 Skyddet för företagshemligheter

3.1 Inledning

I detta kapitel behandlas begreppet företagshemligheter och det rättsliga skyddet av sådana uppgifter. Först genom att definiera vad som utgör en företagshemlighet och sedan den relevanta unionsrättsliga och svenska nationella lagstiftning som reglerar deras skydd. Sådana bestämmelser finns numera i första i direktivet om företagshemligheter som införlivas i svensk nationell rätt genom lagen om företagshemligheter.

3.2 Lagen om företagshemligheter

Under 2016 trädde *Europarlamentets och rådets direktiv 2016/943/EU av den 8 juni om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs* i kraft. Direktivets mål var att stärka skyddet för företagshemligheter och harmonisera detta skydd på EU-nivå för att främja en enhetlig spelplan för företag inom unionen. Direktivet har därefter införlivats i svensk nationell rätt genom lag (2018:558) om företagshemligheter (LFH) som trädde i kraft 1 juli 2018. LFH ersatte lagen (1990:409) om skydd för företagshemligheter från 1990. [65] På internationell nivå har Europeiska unionen och dess medlemssatser sedan 1994 varit bundna av TRIPS-avtalet (Trade-Related Aspects of Intellectual Property Rights) som förhandlades fram inom Världshandelsorganisationen (WTO). [66] TRIPS syftar till att främja innovation och förstärkt konkurrenskraft genom att förhindra snedvridningar inom internationell handel.[67]

Redan vid utredningen för 1990 års lag konstaterades att företagshemligheter utgör en viktig funktion för en välfungerande marknadsekonomi och rättvisa konkurrensförhållanden. Skyddet av nya produktions- och distributionsmetoder genom att hålla viss information hemlig från konkurrenter ger företag betydande fördelar och skapar incitament för investeringar och innovationer. Om skyddsnivån vore för låg skulle Sverige riskera att hamna på efterkälken i den globala utvecklingen. Samtidigt bedömdes skyddet vara tillräckligt balanserat för att inte hindra fri informationsöverföring och konkurrens på marknaden.[68]

Enligt LFH blir lagen endast relevant vid obehöriga angrepp och fungerar i praktiken som ett effektivt rättsligt skydd för arbetsgivaren mot företagsspioneri. Det finns dock ett intresse av att skydda användningen av företagshemligheter för att därigenom främja konkurrensmöjligheter. LFH bygger huvudsakligen på följande intressen:

[65] Christina, Wainikka. *Lagen om företagshemligheter. En kommentar.* Stockholm: JP Infonet, 2023, s. 17.
[66] EUR-Lex, *WTO: avtalet om handelsrelaterade aspekter av immateriella rättigheter*
[67] Wainikka, 2023, s. 26.
[68] SOU 1983:52.

1. Yttrandefriheten som strävar efter att begränsa sekretess och hemlighetsmakeri

2. Marknadsekonomin och den privata äganderätten, som strävar efter att ge näringsidkare största möjliga utrymme för att själva bestämma om egna angelägenheter, inklusive sekretess.

3. Konkurrensrätten, som strävar efter att upprätthålla en sund och lojal konkurrens till nyttjad för konsumenter, andra näringsidkare och samhället i stort.

4. Arbetstagarna, vilkas intresse är att kunna utnyttja sina kunskaper och insikter efter eget gottfinnande.[69]

3.3 Grundläggande begrepp

Lagen om företagshemligheter syftar till att skydda företag mot obehörig anskaffning, användning och röjande av deras hemliga information. Nedan följer en kort genomgång av några av lagens centrala bestämmelser och hur dessa bidrar till skyddet av företagshemligheter.

Det är definitionen av företagshemligheter som utgör själva kärnan i skyddet och det är endast den information som faller inom den definierade ramen för begreppet som är berättigad till skydd.[70] Tidigare lagstiftning definierade ”information” som ”sådana uppgifter som har dokumenterats i någon form, inbegripet ritningar, modeller och andra liknande tekniska förebilder, och enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något särskilt sätt.” Den nuvarande lagstiftningen har tagit bort denna definitionen eftersom den ansågs överflödig.[71] Därmed finns ingen specifik definition av ”information” i 2 § LFH. Informationen kan materialiserats på olika sätt, med digital lagring som den vanligaste formen. Det kan handla om ritningar, prototyper och modeller. Informationen kan även utgöras av ”enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något särskilt sätt”. Detta inkluderar minneskunskaper eller vetskap hos enskilda personer, vilket innebär att anställdas expertis och idéer kan utgöra företagshemligheter.[72] Informationen kan ha olika karaktär och kan avse tekniska, kommersiella eller administrativa förhållanden. Det avgörande är att informationen på något sätt berör näringsidkarens affärs- eller driftförhållanden. Begreppet information omfattar inte bara kommersiella uppgifter om specifika affärshändelser, utan även information om affärshändelser av mer allmän karaktär, som marknadsundersökningar och prissättningskalkyler. Information som kan hänföras till den löpande driften eller produktionen, liksom information som gäller konstruktions- eller utvecklingsarbete, forskning eller liknande verksamheter går också att härleda till information. Begreppet information

[69]Reinhold, Fahlbeck, *Lagen om företagshemligheter. En kommentar och rättsöversikter,* 4 uppl., Stockholm: Norstedts juridik, 2019, s. 42.

[70] Wainikka, 2023, s. 25.

[71] Fahlbeck, 2019, s.383.

[72] Ibid.

i 2 § LFH har därför en av de bredaste möjliga betydelserna och omfattar all information som en näringsidkare vill skydda.[73]

Enligt *JAHAB*-målet förtydligas begreppet information som: ”Ordet information är enligt allmänt språkbruk en samlingsbeteckning för uppgifter, kunskaper och vetande av vilket slag som helst. I begreppet information ryms alltså alla typer av uppgifter oberoende av om de är enkla och okomplicerade eller unika, komplexa eller på annat sätt kvalificerade. Vid lagens tillkomst anfördes att begreppet information har en vidsträckt innebörd och att gränserna för vad som utgör en företagshemlighet sätts av de övriga kriterierna i definitionen samt att ytterligare begränsningar följer av förutsättningarna för ansvar enligt lagen.”[74]

Information som är allmänt känd betraktas inte som företagshemligheter. Kärnan i begreppet är just att information inte är allmänt känd eller lättillgänglig. Sammanställningar som inkluderar uppgifter som är helt eller delvis allmänt kända eller lättillgängliga, kan exempelvis ändå skyddas som företagshemligheter om sammanställningen i sig bedöms vara skyddsvärd.[75] För att avgöra om informationen är allmänt känd eller lättillgänglig tas hänsyn till de åtgärder som innehavaren har vidtagit för att begränsa åtkomsten till informationen. Detta kan inkludera strikta behörighetsbegränsningar och tydliga instruktioner för hur informationen ska hanteras. Enbart det faktum att innehavaren inte har spridit informationen eller att de som har haft tillgång till den borde ha insett att den var konfidentiell är inte tillräckligt för att skydd enligt LFH ska gälla. Innehavaren måste aktivt ha vidtagit konkreta skyddsåtgärder.[76]

Lagen om företagshemligheter gäller endast i situationer där det förekommer obehöriga angrepp på företagshemligheter. Enligt 3 § LFH innebär ett sådant angrepp att någon utan innehavarens samtycker får tillgång till, tillägnar sig, anskaffar, utnyttjar eller röjer företagshemligheten. 4 § LFH klargör att lagens tillämpning är begränsad till dessa specifika situationer.

3.4 Problem med definitionen av ”företagshemligheter”

Internationellt förekommer en mångfald av definitioner när det gäller företagshemligheter, vilket ger lagstiftaren ett brett urval av alternativ att välja mellan. Bristen på enhetliga definitioner mellan olika länder innebär att begreppet företagshemligheter varier mellan olika sammanhang. Dessa skillnader kan innebära att information som anses vara företagshemlighet i en kontext kanske inte får samma skyddsnivå i ett annat sammanhang, Konsekvenserna sträcker sig inte bara till de rättsliga aspekterna vid eventuella intrång på företagshemligheter, utan påverkar även hur olika typer av information behandlas och vilken information som kan delas i affärsrelationer. Trots detta har harmoniseringen inte resulterat i en gemensam

[73] Fahlbeck, 2019, s. 384
[74] NJA 1998 s. 633.
[75] Fahlbeck, 2019, s. 417 f.
[76] Prop. 2017:18/ 200, s. 138 f.

internationell förståelse utanför EU om vad som kan utgöra företagshemligheter, vilket utgör en viktig faktor att beakta vid internationella relationer.[77]

Följden av detta är att definitionen så som den anges i lagtexten är helt avgörande och ofta det som kommer stå i centrum vid rättstvister. Svagheter i lagstiftningen kan helt enkelt leda till att skyddet faller bort helt och hållet. För att uppfylla kraven i definitionen krävs det att man vidtar aktiva åtgärder. En grundläggande princip är att den som önskar skydda företagshemligheter först bör identifiera vilken information som är av sådan betydelse att den ska hanteras på särskilt sätt. Med andra ord är det ett medvetet val att vidta åtgärder för att säkra informationen. Att det är ett val beror på att olika företag gör olika bedömningar, även när det gäller samma typ av information. Vissa aktörer betraktar kundlistor, expansionsplaner och liknande som sina mest värdefulla företagshemligheter, medan andra är mer benägna att dela med sig av dem och kommunicera dem offentligt. Det är alltså inte möjligt att generellt fastställa att en specifik typ av information alltid utgör företagshemligheter. Detta gör att det ställs höga krav på den som vill skydda företagshemligheter att verkligen tydliggöra att något ska hållas hemligt.[78]

Begreppet företagshemlighet definieras i 2§ LFH och innefattar fyra objektiva kriterier:

> ”Med företagshemlighet avses i denna lag information
>
> 1. om affärs- eller driftförhållanden i en näringsidkares rörelse eller i en forskningsinstitutions verksamhet,
>
> 2. som varken som helhet eller i den form dess beståndsdelar ordnats och satts samman är allmänt känd hos eller lättillgängligt för den som normalt har tillgång till information av det aktuella slaget,
>
> 3. som innehavare har vidtagit rimliga åtgärder för att hemlighålla, och
>
> 4. vars röjande är ägnat att medföra skada i konkurrenshänseende för innehavaren”.
>
> Erfarenheter och färdigheter som en arbetstagare har fått vid normal yrkesutövning är inte en företagshemlighet. Inte heller är information om något som utgör ett brott eller annat allvarligt missförhållande en företagshemlighet.”

Bedömningen om viss information utgör en företagshemlighet ska i alla avseenden göras utifrån perspektivet hos den innehavare som påstår att informationen är en företagshemlighet. Utomståendes intressen och åsikter är som regel inte relevanta.[79] En central del av arbetet med att harmonisera skyddet för företagshemligheter inom EU var att etablera en gemensam definition. Definitionen i EU-direktivet liknar den i artikel 39 i TRIPS-avtalet. Båda syftar till att skydda information som har ett kommersiellt värde och som har hållits hemligt av dess ägare.[80] I artikel 2 i direktivet framgår tre centrala krav för att informationen ska beaktas som en företagshemlighet:

1. Informationen är hemlig och inte allmänt känd

[77] Wainikka, 2023, s. 26.
[78] Wainikka, 2023, s. 29.
[79] Fahlbeck, 2019, s. 388.
[80] Wainikka, 2023, s. 27.

2. Informationen har ett kommersiellt värde på grund av att den är hemlig

3. Rimliga åtgärder har vidtagits för att hålla informationen hemlig

Betydelsen av en enhetlig definition betonas ytterligare i skäl 14 i företagshemlighetsdirektivet. Där förklaras att know-how, företagsinformation och teknisk information ska skyddas om de har kommersiellt värde och om olagligt anskaffande, utnyttjande eller röjande av dessa sannolikt skulle skada den person som lagligen kontrollerar informationen. Denna definition omfattar inte obetydlig information eller sådant som är allmänt känt eller lättillgängligt för personer inom de kretsar som normalt hanterar denna typ av information.

4 Samspelet mellan dataskydd och företagshemligheter

4.1 Inledning

I kapitel 2 och 3 har vi gått igenom de grundläggande aspekterna av dataskydd och skyddet för företagshemligheter. Rätten till dataportabilitet innebär att individer har kontroll över sina personuppgifter och kan överföra dem mellan olika tjänsteleverantörer, vilket främjar konkurrensen och användarnas rättigheter. Samtidigt är skyddet för företagshemligheter avgörande för att företag ska kunna bibehålla sina konkurrensfördelar och fortsätta investera i innovation. Personuppgifter har ett stort kommersiellt värde för de flesta företag. Samtidigt finns det ett starkt intresse, särskilt på EU-nivå, att skydda individers personliga integritet från kommersiell användning av deras personuppgifter[81] och att skydda företagshemligheter.[82] Dataportabiliteten kan potentiellt skapa en konflikt mellan dessa intressen, då överföring av personuppgifter ibland kan riskera att avslöja känslig affärsinformation. I detta kapitel kommer vi att undersöka hur dessa två områden samspelar och de potentiella konflikter som kan uppstå.

4.2 Konflikten mellan rätten till dataportabilitet och företagshemligheter

Intressekonflikten mellan utövandet av enskildas rättigheter och skyddet för företagshemligheter har varit föremål för särskild avvägning i ingressen till både GDPR och direktivet om företagshemligheter. Denna av avvägning beskrivs som ”vag” och ”schizofren” i litteraturen [83] vilket gör det relevant att analysera hur dessa två regelverk interagerar.

Skäl 63 i GDPR betonar den registrerades rätt att få tillgång till sina insamlade personuppgifter vilket inkluderar tillgång till information om behandlingen, såsom ändamål, kategorier av personuppgifter lagringstider och mottagare. Denna rättighet syftar till att stärka individens kontroll över sina personuppgifter genom att möjliggöra enkel och regelbunden tillgång. Vidare understryker skäl 63 att dessa rättigheter inte ska påverka andras rättigheter och friheter negativt, särskilt skyddet av affärshemligheter och immateriella rättigheter. Det innebär att, även om individer har rätt till information, ska företagens känsliga affärsinformation och immateriella rättigheter skyddas. Enskilda bör ha rätt att få tillgång till sina personuppgifter på ett enkelt sätt och samtidigt kunna utöva denna rättighet med rimliga intervall. Detta är viktigt för att individer ska kunna bli medvetna om pågående personuppgiftsbehandling och kunna kontrollera lagligheten av dessa. Rätten inkluderar även tillgång till hälsouppgifter, såsom journaldata som innehåller exempelvis diagnoser och undersökningsresultat. Det betonas att enskilda bör informeras om syftet med personuppgiftsbehandlingen, den tidsperiod som

[81] Holtz, Michael Hajo & Ledendal, Jonas, *Överlappningen mellan dataskydd och marknadsrätt*, SvJT, 2020.
[82] Malgieri, Gianclaudio, *Trade Secrets v Personal Data: a possible solution for balancing rights*, International Data Privacy Law, 2016, vol. 6, no. 2, s. 1.
[83] Ibid.

behandlingen förväntas pågå, eventuell automatisk behandling och profilering samt vilka som kommer ta emot uppgifterna.

Intressekonflikten mellan utövandet av enskildas rättigheter och skyddet för företagshemligheter har också behandlats i företagshemlighetsdirektivet. Av skäl 34 och 35 i direktivet framgår att de respekterar de grundläggande rättigheter och principer som erkänns i EU-rättighetsstadga, inklusive rätten till privatliv och skydd av personuppgifter, samtidigt som det skyddar företagshemligheter. Skälen refererar även till GDPR som understryker att företagshemlighetsdirektivet inte bör påverka de enskildas rättigheter och skyldigheter som föreskrivs i förordningen, särskilt rätten till sina personuppgifter. Skälen verkar överensstämma vilket skulle kunna främja ett harmoniskt samspel mellan individers och företags skydd, men vid närmare granskning framkommer en viss osäkerhet som kan ge upphov till konflikter.[84] Å ena sidan bekräftas att företagshemligheter måste beaktas vid utövandet av individers registrerades rättigheter, å andra sidan att registrerades rättigheter måste beaktas vid skyddet av företagshemligheter. Skälen betonar att GDPR:s bestämmelser inte ska inkräkta på skyddet av företagshemligheter och vice versa; skyddet av företagshemligheter ska inte begränsa GDPR:s rättigheter. Denna balansgång kräver noggranna avvägningar i varje enskilt fall för att säkerställa att både registrerades rättigheter och företags intressen skyddas på ett rättvist och effektivt sätt.

Konflikten mellan rätten till dataportabilitet och företagshemligheter aktualiseras särskilt i ljuset av den snabbt växande digitala ekonomin, där data anses vara en av de mest värdefulla tillgångarna för företag.[85] Å ena sidan kan en ökad portabilitet av personuppgifter möjliggöra för användarna att byta mellan olika tjänsteleverantörer och därmed främja konkurrensen på marknaden.[86] Å andra sidan riskerar denna rörlighet att exponera känslig affärsinformation och därmed försvaga företagens konkurrensfördelar.[87] Den ökade möjligheten till dataportabilitet innebär en direkt konflikt med företagens behov av att skydda sina affärshemligheter och konkurrensfördelar. Företag investerar betydande resurser i att samla in och förädla data som utgör kärnan i deras verksamhet. Dessa data kan omfatta exempelvis affärsstrategier och kundinformation, vilket utgör en källa till konkurrensfördelar.[88] I denna kontext uppstår en komplex och motsägelsefull gränsyta där individens rätt till portabilitet balanseras mot företagens intresse av att bevara sina affärshemligheter.

4.3 Överträdelser och ekonomisk påverkan av dataportabilitet

För att förstå hur rätten till dataportabilitet fungerar i praktiken och dess ekonomiska effekter är det viktigt att både analysera överträdelser av GDPR och undersöka hur dessa kan påverka ekonomisk tillväxt och marknadsdynamik.

[84] Ibid.

[85] Svenskt Näringsliv, *EU: s datastrategi och datadelning*, s. 4.

[86] WP 242 rev. 01, s. 4.

[87] Svenskt näringsliv, *EU:s datastrategi och datadelning,* s. 4.

[88] Svenskt Näringsliv, *Avtal om användning av konkurrensklausuler i anställningsavtal, s.* 5.

4.3.1 Överträdelser av dataportabilitetsrätten

I Sverige är Integritetsskyddsmyndigheten (IMY) ansvarig för att säkerställa att företag och organisationer följer GDPR.[89] Artikel 34 i GDPR fastställer hur individer ska informeras om överträdelser, vilket är en del av myndigheternas tillsyn. Ett tydligt exempel på IMY:s arbete är deras sanktionsavgifter mot företag som inte följer GDPR. Ett framträdande fall är Spotify, som fick en betydande avgift för bristande information till sina kunder om hur deras personuppgifter hanterades, vilket bröt mot artikel 12 i GDPR. De specifika överträdelserna omfattade även artiklarna 15–22, som rör den registrerades rättigheter, inklusive rätten till tillgång, rättelse, radering och dataportabilitet. Enligt artikel 15 har den registrerade rätt att få tillgång till sina personuppgifter och information om hur dessa behandlas. IMY fann att Spotify inte tillräckligt tydligt informerade sina användare om hur deras personuppgifter användes, vilket stred mot kraven i artikel 15 samt artikel 34 om informationsskyldigheter vid överträdelser.

IMY utfärdade därför en sanktionsavgift på 58 miljoner kronor mot Spotify. Dessa brister ansågs allvarliga eftersom de påverkade ett stort antal registrerade under en längre tid och försvårade för registrerade att utöva sina rättigheter enligt GDPR. Spotify levererade dessutom personuppgifter för sent och i ett svårtillgängligt format i vissa av fallen, vilket ytterligare bröt mot GDPR:s krav. Detta fall understryker vikten av att företag följer GDPR:s bestämmelser noggrant och tydligt informerar sina kunder om hanteringen av deras personuppgifter.[90] När det gäller böter för bristande efterlevnad av dataportabilitetskraven och andra principer för databehandling visar webbplatsen GDPR Enforcement Tracker att sådana avgifter har utfärdats i stor omfattning. Hittills har dock endast Tjeckien utfärdat en avgift specifikt för överträdelser av rätten till dataportabilitet, och detta vid två tillfällen.[91] Detta indikerar att även om rätten till dataportabilitet är en viktig del av GDPR, är sanktioner direkt kopplade till denna artikel fortfarande relativt ovanliga.

4.3.2 Dataportabilitet och ekonomisk tillväxt

För att den inre marknaden ska fungera effektivt och bidra till ekonomisk tillväxt, innovation och sysselsättning är det avgörande att personuppgifter kan flöda fritt och säkert.[92] I detta syfte har Europeiska kommissionen presenterat en vision för en europeisk dataekonomi där olika aktörer på marknaden samarbetar för att säkerställa tillgängligheten och användbarheten av data över hela EU. Införandet av GDPR syftade till att stödja detta samarbetet genom att skapa en enhetlig tolkning av dataskyddsreglerna inom hela EU. Genom att etablera gemensamma lösningar och tolkningar för företag förväntas GDPR öka förtroendet bland individer och underlätta gränsöverskridande datautbyte.[93] Trots att individens kontroll har framhållits som det främsta syftet med rätten till dataportabilitet, diskuterades även konkurrensaspekten under förberedelserna av GDPR.[94] Även om

[89] Integritetsmyndigheten, *"Om oss",* hämtad 2024-03-22, https://www.imy.se/om-oss/ .

[90] Integritetsmyndigheten, "*Beslut efter tillsyn enligt dataskyddsförordningen – Spotify AB,* 2024-05-01, https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-spotify.pdf.

[91] Enforcement Tracker, *Article 20.*

[92] COM (2012) 9 final, s 2. COM (2017) 9 final, s 1.

[93] COM (2017) 9 final, s 2 f.

[94] CPDP 47/69, "*Making sense of the right to dataportability"*, Computers, Privacy & Data protection Conference, 2016, hämtad 2024-04-20, https://www.youtube.com/watch?v=yy7qfWjyCUM.

konkurrensregleringen inte ingår direkt i GDPR, är det fria flödet av data och främjandet av ekonomisk tillväxt centrala principer inom EU:s dataskyddslagstiftning.[95]

Rätten till dataportabilitet innebär att användare kan flytta sina personuppgifter mellan olika tjänsteleverantörer, vilket begränsar leverantörernas möjlighet att använda inläsning av dessa som ett otillbörligt konkurrensmedel. Dataportabiliteten betonar att företag inte äger individers personuppgifter, istället har individer full rådighet över sin data och kan överföra den till en annan plattform vid behov. Detta ger individen en frihet att agera och hjälper till att balansera maktförhållandet mellan individen och tjänsteleverantörer, vilket stärker individens roll på marknaden.[96] Dataportabiliteten förväntas därför inte bara öka konkurrensen mellan olika tjänsteleverantörer utan också främja en mer effektiv samhällsekonomin.[97] Ökad konkurrens pressar företag att förbättra sina tjänster och produkter för att behålla och attrahera kunder, vilket i sin tur kan leda till ökad innovation och effektivitet. Dataportabiliteten kan ses som ett verktyg för att främja en sund konkurrens och en dynamisk ekonomisk miljö genom att möjliggöra en smidig överföring av personuppgifter mellan olika tjänsteleverantörer.

[95] WP 242 rev. 01, s 4.
[96] WP 242 rev. 01, s. 4.
[97] SOU 2017:52, s. 44.

5 Sammanfattning och slutsatser

Syftet med uppsatsen har varit att beskriva och analysera samspelet mellan rätten till dataportabilitet i EU:s dataskyddsförordning och skyddet för företagshemligheter enligt företagshemlighetsdirektivet. Uppsatsens frågeställningar lyder följande:

- Vad innebär rätten till dataportabilitet i EU:s dataskyddsförordning?
- Vad menas med företagshemligheter och vilket skydd får dessa enligt lagen om företagshemligheter?
- Hur begränsas rätten till dataportabilitet av skyddet för företagshemligheter?

Rätten till dataportabilitet var en nyhet bland GDPR:s bestämmelser när den blev tillämplig 2018. Dataportabiliteten ger individer rätten att få ut sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format samt att kunna överföra dessa uppgifter till en annan personuppgiftsansvarig. Syftet med dataportabiliteten är att stärka individens kontroll över sina egna uppgifter och underlätta förflyttningen av data mellan olika tjänsteleverantörer.

Skyddet för företagshemligheter, som regleras av företagshemlighetsdirektivet och LFH i svensk kontext, syftar till att skydda företagens känsliga affärsinformation från att utnyttjas av konkurrenter eller spridas vidare. GDPR och företagshemlighetsdirektivet tar upp två viktiga, men i vissa fall motstridiga intressen, skyddet av individers rätt till dataportabilitet och skyddet av företagshemligheter. Dessa regelverk försöker balansera dessa intressen genom att etablera specifika riktlinjer och bestämmelser för hur dessa rättigheter ska hanteras.

Skäl 63 i GDPR betonar att utövandet av rätten till tillgång och andra rättigheter inte får negativt påverka andras rättigheter och friheter, inklusive skyddet för företagshemligheter och immateriella rättigheter. Skälet klargör att det finns ett behov av att balansera individens rätt till personuppgifter med företagens behov av att skydda känslig information. Skäl 34 och 35 i företagshemlighetsdirektivet betonar skyddet av grundläggande rättigheter och principer som respekt för privatliv och skydd av personuppgifter. Dessa skäl understryker att skyddet av företagshemligheter inte bör påverka de rättigheter och skyldigheter som finns i GDPR. Tillsammans visar dessa skäl en tydlig strävan att harmonisera de två regelverken och skapa en rättvis balans mellan individers och företags intressen. Det framgår att både GDPR och företagshemlighetsdirektivet erkänner behovet av att skydda personuppgifter och företagshemligheter, men de betonar också att ingen av dessa rättigheter ska ha företräde framför den andra. Detta indikerar en gemensam ambition att säkerställa att rättigheter och friheter skyddas på ett balanserat sätt, viket är avgörande för att upprätthålla både rättssäkerhet och ekonomisk tillväxt inom EU. Vid en verklig konflikt mellan rätten till dataportabilitet och skyddet för företagshemligheter blir det avgörande att klargöra vad som utgör företagshemligheter. Det är ofta oklart vad som faktiskt utgör företagshemligheter, medan GDPR tydligt anger de rättigheter och krav som följer av förordningen.

Företag måste vara väl förberedda att identifiera och skydda sina företagshemligheter samtidigt som de uppfyller kravet på dataportabilitet.

GDPR har förändrat hur företag arbetar genom att införa strikta regler för hur data ska samlas in, lagras och delas. Genom att införa dessa regler har GDPR stärkt individers rättigheter och säkerställt en högre nivå av dataskydd. Samtidigt har lagen beaktat möjliga konflikter mellan skyddet av företagshemligheter och individers rättigheter. Trots detta är det oklart hur gränserna ska dras och hur reglerna ska tillämpas i praktiken. Företag står inför flera utmaningar när det gäller att balansera skyddet av företagshemligheter med individens rätt till dataportabilitet och dataskydd. Trots att GDPR inkluderar rätten till dataportabilitet, och att tillsynsmyndigheter har utfärdat sanktionsavgifter för att företag har misslyckats att tillgodose andra rättigheter inom GDPR, återfinns få exempel i praxis på bristande hantering av dataskyddsansvariga i relation till artikel 20. Detta kan bero på flera faktorer. För det första är det svårt för individer och tillsynsmyndighet att påpeka för företag att de inte uppfyller kraven tillräckligt bra, eftersom det finns en komplex konfliktyta mellan att möjliggöra dataportabilitet och samtidigt skydda företagshemligheter. Företag kan vara ovilliga att implementera full dataportabilitet av rädsla för att känslig information ska avslöjas eller missbrukas. För det andra kan bristen på tydliga rättsfall och annan rättspraxis göra det svårt för företag att veta exakt hur de ska tillämpa artikel 20, vilket leder till osäkerhet och ibland kanske till och med undvikande av att implementera denna rättighet.

Diskussionen kring bristen på rättsfall är relevant. Vid GDPR:s intåg var det mycket uppmärksamhet och debatt kring lagens olika aspekter. Trots att artikel 20 var en nyhet i förordningen verkar den ha hamnat i skymundan. Det är svårt att säga exakt varför, men det kan bero på att människor, trots lagens bestämmelser, inte alltid är medvetna om sina rättigheter eller helt enkelt inte bryr sig om att utnyttja dem. I en redan konkurrensdriven marknad som EU:s, är det kritiskt att dessa rättigheter och skydd tillämpas och värderas korrekt.

Sammanfattningsvis kan vi säga att medan GDPR har satt en hög standard för dataskydd, återstår det arbete för att säkerställa att alla dess aspekter, inklusive rätten till dataportabilitet enligt artikel 20, uppfylls och implementeras på ett sätt som balanserar både individers rättigheter och skyddet av företagshemligheter. Företagshemligheter utgör en betydande tillgång för företag och måste skyddas för att säkerställa affärsframgång och innovation. Denna konflikt är troligen bara i sin början, och motsättningarna mellan datainsamling och personlig integritet lär fortsätta väcka debatt framöver. Vilket av dessa två intressen som bör väga tyngst kommer sannolikt att vara en fråga om tolkning, ofta färgad av politiska skiljelinjer.

Att uppnå en rättvis balans mellan att skydda företagshemligheter och att respektera individers rättigheter kommer dock framöver att vara avgörande för att upprätthålla rättssäkerhet, främja innovation och främja en dynamisk och konkurrenskraftig marknad inom EU.

Källförteckning

Offentligt tryck

Sverige

Statens offentliga utredningar

SOU 2017:52 Så stärker vi den personliga integriteten

SOU 1983:52 Företagshemligheter

Propositioner

Prop. 2017:18/ 200 En ny lag om företagshemligheter

Svensk lagstiftning

Lag (2018:558) om företagshemligheter, som trädde i kraft den 1 juli 2018, genomför Europaparlamentets och rådets direktiv (EU) 2016/943 om skydd för företagshemligheter mot olovligt förvärv, användning och röjande. (Cit: lagen om företagshemligheter).

Europeiska unionen

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) (EUT L119, 04.05.2016). (Cit: GDPR).

Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L157, 15.06.2016). Cit: företagshemlighetsdirektivet).

Meddelande från kommissionen

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska sociala kommitté samt Regionkommittén, Skydd av den personliga integriteten i en uppkopplad värld, En europeisk ram för personuppgiftsskydd för tjugohundratalet, 2012-01-25, COM (2012) 9 final.

Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska och sociala kommittén samt Regionkommittén, Att skapa en europeisk dataekonomi, 2017-01-10, COM (2017) 9 final.

Artikel 29-gruppen

Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 2016-12-13.

Litteratur

Doktrin

Bernitz, U., Bernitz, H., Carlsson, M., Heuman, L., Leijonhufvud, M., Magnusson Sjöberg, C., Seipel, P., Warnling Conradson, W., Vogel. H-H. *Finna rätt: Juristens källmaterial och arbetsmetoder.* 16 uppl. Norstedt Juridik AB, 2023.

Fahlbeck, Reinhold. *Lagen om företagshemligheter. En kommentar och rättsöversikter.* 4 uppl. Stockholm: Norstedt Juridik AB, 2019.

Frydlinger, D., Edvardsson, T., Olstedt Carlström, C., Beyer, S. *GDPR. Juridik, organisation och säkerhet enligt dataskyddsförordningen.* Norstedt Juridik AB, 2018.

Gianclaudio Malgieri, *Trade Secrets v Personal Data: a possible solution for balancing rights, International Data Privacy Law,* 2016, vol. 6, no. 2.

Gunnarsson, Åsa. & Svensson, Eva-Maria. *Rättsdogmatik – som rättsvetenskapligt perspektiv och metod*. Lund: Studentlitteratur AB, 2023.

Hettne, Jörgen. & Eriksson Otken, Ida. *EU-rättslig metod. Teori och genomslag i svensk rättstillämpning.* 2 uppl. Stockholm: Norstedt Juridik AB, 2011.

Holtz, Michael Hajo & Ledendal, Jonas, *Överlappningen mellan dataskydd och marknadsrätt*, SvJT, 2020.

Kleineman, Jan. Rättsdogmatisk metod. *Juridisk metodlära*. I Nääv, Maria & Zamboni Mauro (red.). 2 uppl. Lund: Studentlitteratur AB, 2018.

Wainikka, Christina. *Lagen om företagshemligheter. En kommentar.* Stockholm: JP Infonet AB, 2023.

Öman, Sören. *Dataskyddsförordningen (GDPR) m.m. En kommentar.* 2 uppl. Stockholm: Norstedt Juridik AB, 2021.

Tidskrift

Holtz, Michael Hajo & Ledendal, Jonas, *Överlappningen mellan dataskydd och marknadsrätt*, SvJT, 2020.

Internetkällor

CPDP 47/69, "*Making sense of the right to dataportability"*, Computers, Privacy & Data protection Conference, 2016, hämtad 2024-04-20, https://www.youtube.com/watch?v=yy7qfWjyCUM

GDPR Enforcement Tracker, "*Article 20",* hämtad 2024-05-03, *https://enforcementtracker.com*

Europeiska unionen (EU), ”*Trade secrets”,* Europa.eu, hämtad 2024-04-22 https://europa.eu/youreurope/business/running-business/intellectual-property/trade-secrets/index_en.htm hämtad 2024-05-03

Integritetsmyndigheten,” *Ordlista – Personuppgifter”*, hämtad 2024-03-27, *https://www.imy.se/ordlista/#P*

Integritetsmyndigheten, *”Om oss”*, hämtad 2024-03-22, https://www.imy.se/om-oss/

Integritetsmyndigheten, *” Beslut efter tillsyn enligt dataskyddsförordningen – Spotify AB,* hämtad 2024-05-01, https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-spotify.pdf

Integritetsmyndigheten, ”*Grundläggande principer”*, hämtad 2024-04-01 https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

Integritetsmyndigheten, ”*Den registrerades rättigheter”*, hämtad 2024-04-01, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/de-registrerades-rattigheter/

Integritetsmyndigheten, ”*Personuppgiftsansvariga och personuppgiftsbiträden”*, hämtad 2024-04-05, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/

Svenskt näringsliv, ”*EU:s datastrategi och datadelning”*, hämtad 2024-05-06*,* https://www.svensktnaringsliv.se/bilder_och_dokument/rapporter/knrkls_eus_datastrategi_och_datadelning_webben_pdf_1164894.html/EUs_datastrategi_och_datadelning_webben_.pdf

Svenskt näringsliv, ”*Avtal om användning av konkurrensklausuler i anställningsavtal”*, hämtad 2024-05-10, https://www.ptk.se/wp-content/uploads/2021/04/Svenskt-Naringsliv-PTK-2015-Avtal-Konkurrensklausuler-1.pdf

Rättsfall

Högsta domstolen

NJA 1998 s. 633