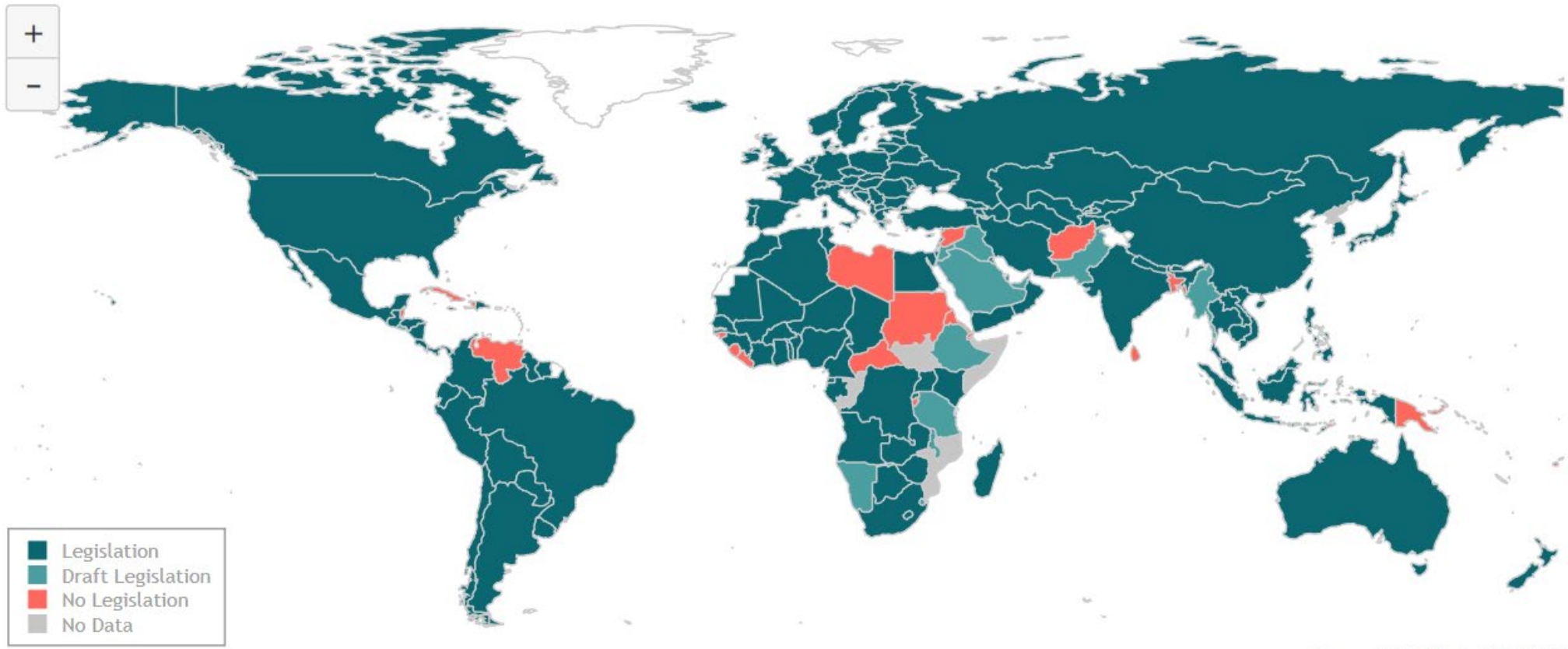
Dataskydd

Grundläggande terminologi m.m.

Anne Savolainen, jurist Karolinska Universitetssjukhus

KAROLINSKA UNIVERSITETSSJUKHUSET

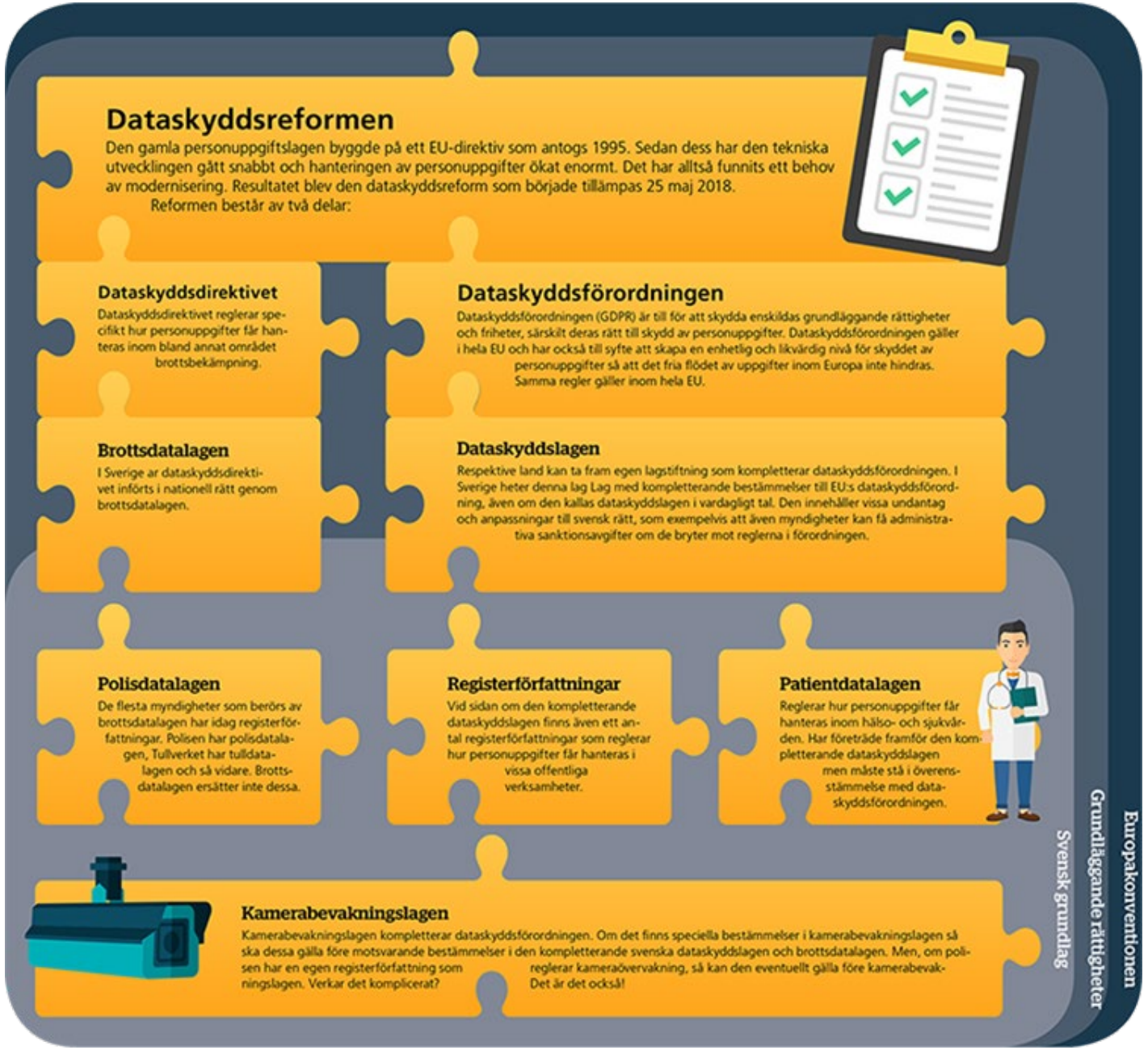
Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

Var regleras dataskydd?

I Sverige:



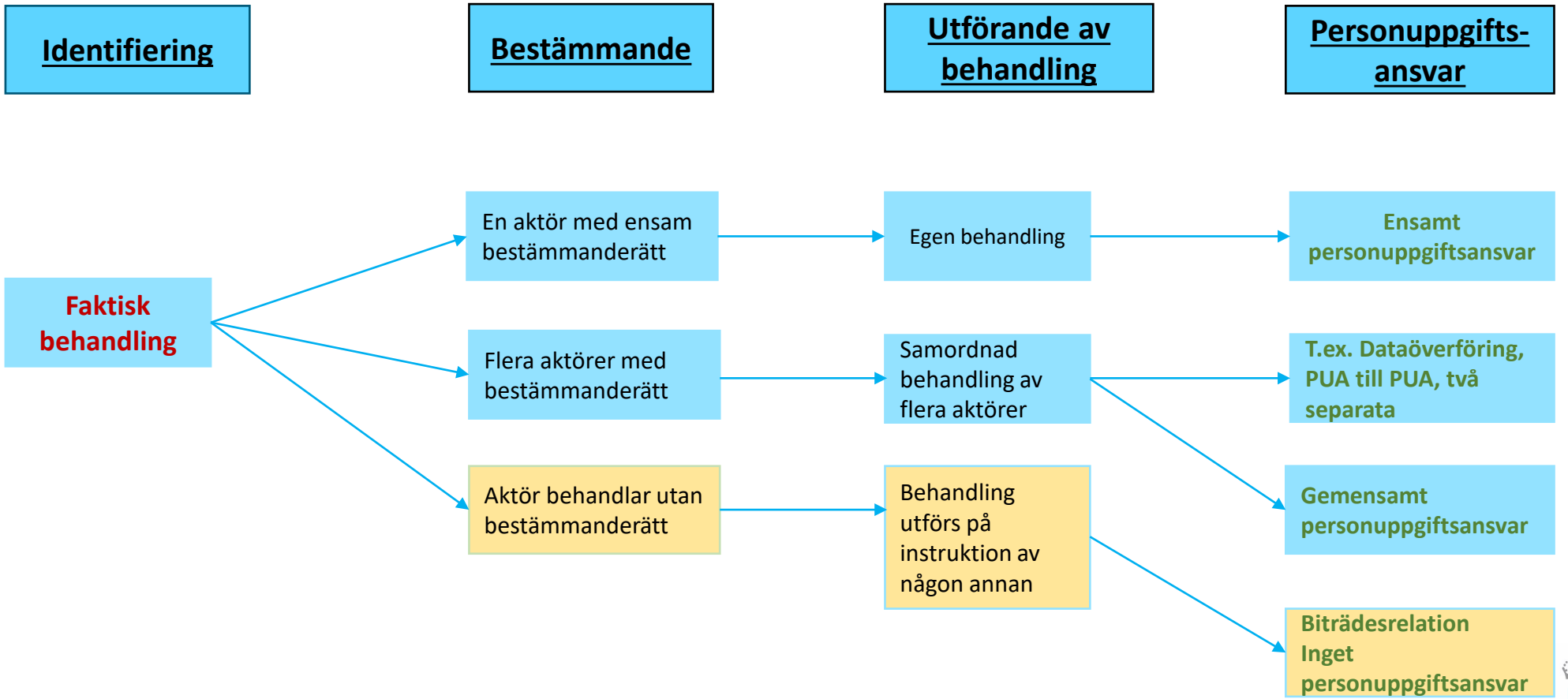
Ansvar för personuppgiftsbehandling

- En aktör som behandlar personuppgifter kan antingen vara
  - personuppgiftsansvarig
  - personuppgiftsbiträde.

- Personuppgiftsansvaret kan bäras av
  - en aktör ensamt
  - flera aktörer gemensamt.
- En personuppgiftsansvarig har
  - bestämmanderätt över ändamålen och medlen för behandlingen
  - skyldigheter att behandla personuppgifter enligt lag och annan regelverk.

- Mellan två eller fler aktörer som behandlar personuppgifter finns tre möjliga relationer i enlighet med GDPR:
  - Två personuppgiftsansvariga med separat ansvar,
  - Två personuppgiftsansvariga med ett gemensamt ansvar, eller
  - En/eller flera personuppgiftsansvarig och ett/eller flera personuppgiftsbiträde.

Ansvarskedjan



Behandling av PU

- Behandling, art. 4 p. 2
  en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgif
  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
  - ✓ sammanförande, begränsning
  - ✓ radering eller förstöring
- Beskriv dataflöden och aktörerna (om möjligt)
- Identifiera och beskriv personuppgiftsbehandlingar
- Beskriv varför uppgiften behöver behandlas, dvs. ändamålet med behandlingen. Hänvisa till ev. lagrum.
  - ➢ uppgifter samlas för forskningsändamål
  - ➢ uppgifterna bearbetas i en forskningsstudie
  - ➢ Efter avslutat studie sparas/arkiveras uppgifter x antal år
  - ➢ därefter ska uppgifterna raderas

Vad är personuppift?

- Varje upplysning som avser en identifierad eller identifierbar fysisk person
- Kan identifieras
  - direkt
  - Indirekt

- Pseudonymiserade personuppgifter behandlats på ett sätt som innebär att de inte längre kan tillskrivas
  - en specifik individ
  - utan att använda kompletterande uppgifter
  - kompletterande uppgifter förvaras separat
  - skyddas av åtgärder som säkerställer att de inte kan användas för att identifiera individen. ’
  - möjlighet att länka till individen

- Blanda inte ihop med anonymisering.
  - Inte längre möjlighet att länka till individen på något sätt

Avidentifierade, pseudonymiserade och anonymiserade personuppgifter

Tabell med direkta och indirekta personuppgifter, t.ex. inom vården.

Namn	Kön	Födelsedata	Vikt	Längd
Anna	Kvinna	19651031	63	165
Kalle	Man	19680818	91	181
Ellen	Kvinna	19710322	71	173
Peter	Man	19740130	80	178

Avidentifiering av personuppgifter i tabellen, t.ex. verksamhetsuppföljning, behov att ha ”individer”.

Namn	Kön	Födelsedata	Vikt	Längd
	Kvinna	19x51x3x	63	165
	Man	19x80x1x	91	181
	Kvinna	19x10x2x	71	173
	Man	19x40x3x	80	178

Avidentifierade, pseudonymiserade och anonymiserade personuppgifter

Pseudonymisering av personuppgifter i tabellen, t.ex. forskningsstudie

Namn	Kön	Födelsedata	Vikt	Längd
P1	Kvinna	19651031	63	165
P2	Man	19680818	91	181
P3	Kvinna	19710322	71	173
P4	Man	19740130	80	178

Anonymisering av tabellen, t.ex. statistiska uppgifter

Namn	Kön	Ålder	Vikt	Längd
	Kvinna	>50 <60	>60 <70	>160 <170
	Man	>50 <60	>90 <100	>180 <190
	Kvinna	>50 <60	>70 <80	>170 <180
	Man	>40 <50	>80 <90	>170 <180

PUA behöver **en rättslig grund** för behandling

- Art 6.1
- a) Samtycke
- b) Fullgörande av avtal
- c) Rättslig förpliktelse
- d) Vitala intressen
- e) Allmänt intresse
- f) Berättigat intresse

- Särskilda kategorier av personuppgifter, känsliga personuppgifter
- -> **Huvudregel** behandling förbjudet

- Art. 9.1
  - Ras/etnisk ursprung
  - Politiska åsikter
  - Religiös eller filosofisk övertygelse
  - Medlemskap i fackförening
  - Genetiska uppgifter
  - Biometriska uppgifter för att identifiera fysisk person
  - Uppgifter om hälsa
  - Uppgifter om sexualliv och sexuell läggning

Undantag från förbjudet i art. 9.1.

- Art. 9.2
- a) Samtycke
- b) Nödvändig ska PUA eller registrerade ska kunna fullgöra sina skyldigheter och rättigheter inom arbetsrätten
- c) För att skydd någons grundläggande intressen
- d) Berättigad verksamhet hos stiftelse, förening eller icke vinstdrivande organisation som har politiskt, filosofiskt, religiöst el. fackligt syfte
- e) Uppgifter har offentliggjorts av registrerade
- f) Nödvändig för att fastställa rättslig anspråk eller del av domstolarnas dömande verksamhet
- g) Behandlingen är viktigt i hänsyn till viktigt allmänt intresse kopplat till nationell rätt eller unionsrätten
- h) Nödvändig behandling inom hälso- och sjukvård och socialomsorg
- i) Allmänt intresse inom folkhälsoområdet
- j) Arkivändamål av allmänt intresse, vetenskapliga och historiska forskningsändamål

- Art. 9.3
- Uppgifter enligt art. 9.2 h) Får behandlas av dem som omfattas av tystnadsplikt

Personuppgiftsansvar

1) Personuppgifter behandlas av ensamt av en aktör med eget bestämmande/krav i lag. T.ex. efter datauttag av en annan personuppgiftsansvarig, forskning görs på eget data, samlas in från patienten själv

➢ **Ensamt personuppgiftsansvar**

2) Personuppgifter behandlas samordnat/koordinerat av flera aktörer men parterna agerar vid sidan av varandra. T.ex. data samlas in i en klinisk läkemedelsstudie och lämnas till ett läkemedelsföretag som utvecklar läkemedlet, data behandlas av olika aktörer som agerar samordnat men har eget ansvar enligt lag för behandling t.ex. vårdgivaransvar, personalansvar e.d. Ett remissförfarande är också exempel på en situation under denna punkt.

➢ **Två separata personuppgiftsansvar**

3) Personuppgifter behandlas samordnat/koordinerat/tillsammans av flera aktörer som agerar gemensamt. T.ex. en studie där flera parter forskar gemensamt på det insamlade datat, när parter samordnar lagring t.ex. efter en forskningsstudie.

➢ **Gemensamt personuppgiftsansvar**

4) Behandlas personuppgifter för någon annans räkning som är ansvarig

➢ **Personuppgiftsbiträde**

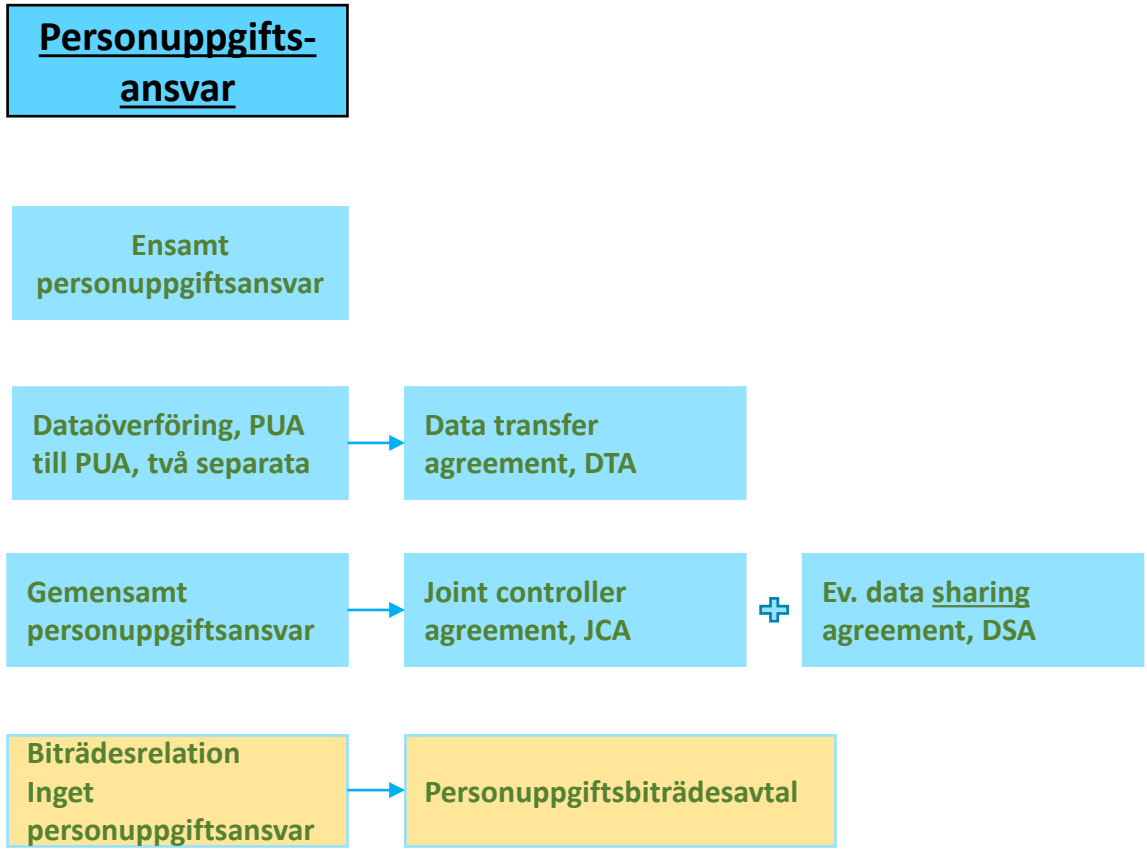
T.ex. ett forskningslaboratorium som inte är vårdgivare,

- dvs. resultaten används inte för vården av patienten
- dvs. det finns inte krav på (egen) behandling enligt lag hos laboratoriet

➢ Skilj från ett laboratorium som tar prover på remiss och resultaten ska användas i den kliniska vården av patienten. Då är laboratoriet en vårdgivare. Vårdgivare har krav på journalföring enligt lag **-> laboratoriet har eget personuppgiftsansvar** (se p. 4)

Sjukhuset kan i princip aldrig vara biträde då man som vårdgivare har ansvar för journalföring, patientens vård e.d.

Avtal som följd av faktisk behandling



Överföring till tredje land

- Innebär överföring av personuppgifter till tredje land innebär att personuppgifter behandlas eller är tänkt att behandlas i ett land utanför EU/EES-området. Art. 44.

- Räcker att personuppgifterna blir tillgängliga för någon i ett land utanför EU/EES-området.

- **Tillåtet i vissa fall, men reglerna är strikta.**

- <u>Varför?</u>
- Genom dataskyddsförordningen har alla EU:s medlemsstater ett likvärdigt skydd för personuppgifter och personlig integritet.
- -> personuppgifter kan föras över fritt inom detta område utan begränsningar.

- Utanför EU/EES däremot finns inga generella regler som ger motsvarande garantier.

Förutsättningar för överföring till tredje land

- Art. 45
- Adekvat skyddsnivå, beslut av EU-kommissionen
- Andorra
- Argentina
- Bailiwick of Guernsey
- Färöarna
- Isle of Man
- Israel
- Japan
- Jersey
- Nya Zeeland
- Schweiz
- Storbritannien
- Sydkorea
- Uruguay

EU-kommissionen bedömt att skyddsnivån är adekvat under särskilda villkor i följande länder:

- **Kanada**, om lagstiftning i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.
- **USA**, om mottagaren omfattas av ”EU-US Data Privacy Framework”.

- Art. 46
- Om den personuppgiftsansvariga vidtar lämpliga skyddsåtgärder:
- Bindande företagsbestämmelser
- Standardavtalsklausuler som EU-kommissionen har beslutat om, SSC
- Godkända uppförandekoder eller certifieringsmekanismer
- Rättsligt bindande instrument mellan myndigheter.

- *Det måste dessutom finnas lagstadgade rättigheter och möjlighet för de registrerade att klaga på personuppgiftsbehandlingen och få den prövad i domstol.*

Standard avtalsklausuler, standrad contractual clauses, SCC

- Godkänns av kommissionen
- Får inte ändras men möjligt att lägga till affärsrelaterade klausuler om de inte strider mot andra klausuler.
- Innehåller skyldigheter dels för PUA som vill föra över personuppgifter till länder utanför EU/EES, dels för PUA eller PUB som tar emot sådana uppgifter.
- Reglerar också andra frågor kring överföringen, till exempel de registrerades rättigheter och hur tvister med anledning av avtalet ska lösas.
- Kraven i artikel 28.3 GDPR integrerats, vilket innebär att parterna inte längre behöver ingå något separat PUB-avtal.
- Flera parter att ansluta sig till samma avtal.
- Alternativ:
  - (i) PUA till PUA
  - (ii) PUA till PUB
  - (iii) PUB till PUB
  - (iv) PUB till PUB

Avtal för att regler tredjelandsöverföring