

ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER



17/SV

WP 248 rev. 01

Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679

Antagna den 4 april 2017

Senast reviderade och antagna den 4 oktober 2017

Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet. Dess uppgifter beskrivs i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

Gruppens sekretariat finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) på Europeiska kommissionen, Generaldirektoratet för rättsliga frågor, B-1049 Bryssel, Belgien, Kontor MO-59 03/075.

Webbplats: http://ec.europa.eu/justice/data-protection/index_en.htm

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV PERSONUPPGIFTER HAR

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995, genom vilket arbetsgruppen inrättades,

med beaktande av artiklarna 29 och 30 i detta direktiv,

med beaktande av sin arbetsordning

ANTAGIT FÖLJANDE RIKTLINJER:

Innehållsförteckning

I.	INLEDNING.....	4
II.	RIKTLINJERNAS TILLÄMPNINGSOMRÅDE	5
III.	KONSEKVENSBEDÖMNING: FÖRKLARINGAR TILL FÖRORDNINGEN.....	7
A.	VAD SKA EN KONSEKVENSBEDÖMNING HANTERA? EN ENDA BEHANDLING ELLER EN SERIE LIKNANDE BEHANDLINGAR.	8
B.	VILKA BEHANDLINGAR ÄR FÖREMÅL FÖR EN KONSEKVENSBEDÖMNING? FÖRUTOM VID UNDANTAG, NÄR DE "SANNOLIKT LEDER TILL EN HÖG RISK".	9
a)	När är det obligatoriskt med en konsekvensbedömning? När behandlingen "sannolikt leder till en hög risk". 9	
b)	När krävs det inte en konsekvensbedömning? Om behandlingen inte "sannolikt leder till en hög risk", eller det finns en liknande konsekvensbedömning, eller den har godkänts före maj 2018, eller har en rättslig grund, eller finns med i förteckningen över behandlingar som inte kräver en konsekvensbedömning.	14
C.	VAD GÄLLER FÖR REDAN BEFINTLIGA BEHANDLINGAR? KONSEKVENSBEDÖMNINGAR KRÄVS UNDER VISSA OMSTÄNDIGHETER.	15
D.	HUR SKA EN KONSEKVENSBEDÖMNING UTFÖRAS?	16
a)	Vid vilken tidpunkt ska en konsekvensbedömning utföras? Före behandlingen.	16
b)	Vem är skyldig att utföra konsekvensbedömningen? Den personuppgiftsansvarige, tillsammans med dataskyddsombudet och personuppgiftsbiträdena.....	16
c)	Vilken metod ska användas för att utföra en konsekvensbedömning? Olika metoder men gemensamma kriterier.	17
d)	Är det obligatoriskt att offentliggöra konsekvensbedömningen? Nej, men genom ett offentliggörande av sammanfattningen kan förtroende skapas. Den fullständiga konsekvensbedömningen ska meddelas tillsynsmyndigheten i fall av förhandssamråd eller om dataskyddsmyndigheten så begär.....	21
E.	NÄR SKA TILLSYNSMYNDIGHETEN RÅDFRÅGAS? NÄR DEN KVARSTÅENDE RISKEN ÄR HÖG.	21
IV.	SLUTSATSER OCH REKOMMENDATIONER	22
	BILAGA 1 – EXEMPEL PÅ BEFINTLIGA RAMVERK FÖR KONSEKVENSBEDÖMNING I EU	24
	BILAGA 2 – KRITERIER FÖR EN GODTAGBAR KONSEKVENSBEDÖMNING	25

I. Inledning

Förordning 2016/679¹ (nedan kallad *förordningen*) gäller från och med den 25 maj 2018. Genom artikel 35 i förordningen införs begreppet ”konsekvensbedömning avseende dataskydd” (nedan kallad *konsekvensbedömning*²), liksom genom direktiv 2016/680³.

En konsekvensbedömning är en process avsedd att beskriva behandlingen, bedöma huruvida den är nödvändig och proportionell och hjälpa till att hantera risker för fysiska personers rättigheter och friheter som uppkommer genom behandlingen av personuppgifter⁴ genom att bedöma dem och bestämma vilka åtgärder som ska vidtas. Konsekvensbedömningar är viktiga verktyg för utkrävande av ansvar, eftersom de inte bara hjälper personuppgiftsansvariga att uppfylla kraven i förordningen, utan även visar att lämpliga åtgärder har vidtagits för att säkerställa efterlevnaden av förordningen (se även artikel 24)⁵. Med andra ord **är en konsekvensbedömning en process för att skapa och påvisa efterlevnad.**

Enligt förordningen kan underlåtelse att iaktta kraven på konsekvensbedömning leda till att behörig tillsynsmyndighet utkräver sanktionsavgifter. Underlåtelse att utföra en konsekvensbedömning när behandlingen är föremål för en konsekvensbedömning (artikel 35.1 och 35.3–4), utförande av en konsekvensbedömning på ett felaktigt sätt (artikel 35.2 och 35.7–9), eller underlåtelse att samråda med behörig tillsynsmyndighet om detta krävs (artikel 36.3 e), kan medföra en administrativ

¹ 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).

² I andra sammanhang används ofta begreppet ”konsekvensbedömning avseende integritet” för att hänvisa till samma koncept.

³ I artikel 27 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter föreskrivs även att en konsekvensbedömning avseende dataskydd behövs om ”behandling[en] [...] sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

⁴ I förordningen definieras inte begreppet konsekvensbedömning i sig i formellt hänseende, men

- dess minimiinnehåll specificeras på följande sätt i artikel 35.7:
 - o ”a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
 - o b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
 - o c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och
 - o d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.”
- dess innebörd och roll klargörs på följande sätt i skäl 84: ”I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende dataskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar.”

⁵ Se även skäl 84: ”Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning.”

sanktionsavgift på upp till 10 miljoner euro, eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

II. Riktlinjernas tillämpningsområde

Dessa riktlinjer tar hänsyn till

- yttrande 14/EN WP 218⁶ från artikel 29-arbetsgruppen (nedan kallad *arbetsgruppen*),
- arbetsgruppens riktlinjer om dataskyddsbud 16/EN WP 243⁷,
- arbetsgruppens yttrande om ändamålsbegränsningar 13/EN WP 203⁸,
- internationella standarder⁹.

I överensstämmelse med den riskbaserade metoden i förordningen är det inte obligatoriskt att utföra en konsekvensbedömning för varje behandling. En konsekvensbedömning krävs endast om behandlingen ”*sannolikt leder till en hög risk för fysiska personers rättigheter och friheter*” (artikel 35.1). För att säkerställa en enhetlig tolkning av de situationer i vilka en konsekvensbedömning är obligatorisk (artikel 35.3) är det huvudsakliga syftet med de aktuella riktlinjerna att klargöra detta begrepp och tillhandahålla kriterier för de förteckningar som dataskyddsmyndigheterna ska upprätta enligt artikel 35.4.

Enligt artikel 70.1 e kan Europeiska dataskyddsstyrelsen utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av förordningen. Syftet med detta dokument är att föregå ett sådant framtida arbete från Europeiska dataskyddsstyrelsen och klargöra de aktuella bestämmelserna i förordningen för att hjälpa personuppgiftsansvariga att följa lagen och skapa rättssäkerhet för personuppgiftsansvariga som är skyldiga att utföra en konsekvensbedömning.

Dessa riktlinjer har även i syfte att främja utvecklingen av

- en gemensam europeisk förteckning över det slags behandlingsverksamheter som omfattas av kravet på konsekvensbedömning (artikel 35.4),
- en gemensam EU-förteckning över det slags behandlingsverksamheter som inte behöver någon konsekvensbedömning (artikel 35.5),
- gemensamma kriterier för de metoder som används för att utföra en konsekvensbedömning (artikel 35.5),
- gemensamma kriterier för att specificera när samråd ska genomföras med tillsynsmyndigheten (artikel 36.1),

⁶ Arbetsgruppens yttrande 14/EN WP 218 *Statement on the role of a risk-based approach in data protection legal frameworks* (Yttrande om en riskbaserad metod inom den rättsliga ramen för uppgiftsskydd), antaget den 30 maj 2014.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

⁷ Arbetsgruppens riktlinjer om dataskyddsbud 16/EN WP 243, antagna den 13 december 2016.

http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

⁸ Arbetsgruppens yttrande 03/2013 om ändamålsbegränsningar 13/EN WP 203, antaget den 2 april 2013.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

⁹ T.ex. ISO 31000:2009, *Riskhantering – Principer och riktlinjer*, Internationella standardiseringsorganisationen (ISO), ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Internationella standardiseringsorganisationen (ISO).

- rekommendationer som, om möjligt, bygger på erfarenheter som fåtts i medlemsstaterna.

III. Konsekvensbedömning: förklaringar till förordningen

Enligt förordningen är personuppgiftsansvariga skyldiga att genomföra lämpliga åtgärder för att säkerställa och för att kunna visa att förordningen efterlevs, bland annat med beaktande av ”riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter” (artikel 24.1). Skyldigheten för personuppgiftsansvariga att i vissa fall utföra en konsekvensbedömning bör tolkas mot bakgrund av deras allmänna skyldighet att på ett lämpligt sätt hantera de risker¹⁰ som uppkommer vid behandling av personuppgifter.

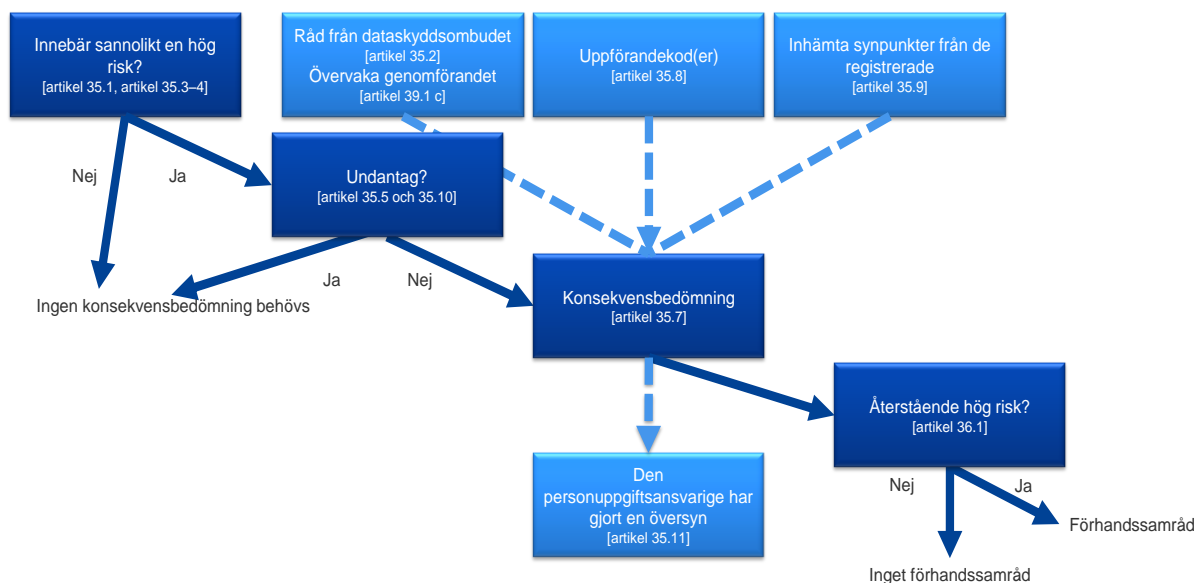
En ”risk” är ett scenario som beskriver en händelse och dess uppskattade konsekvenser vad gäller allvar och sannolikhet. ”Riskhantering” däremot, kan definieras som en samordnad verksamhet för att styra och kontrollera en organisation med avseende på risk.

I artikel 35 hänvisas till en sannolikt hög risk ”för enskildas rättigheter och friheter”. Såsom anges i yttrandet från artikel 29-arbetsgruppen för skydd av personuppgifter om den riskbaserade metoden inom den rättsliga ramen för uppgiftsskyddet avser hänvisningen till de registrerades ”rättigheter och friheter” i första hand dataskydd och integritet, men kan även omfatta andra grundläggande rättigheter såsom yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion.

I överensstämmelse med den riskbaserade metoden i förordningen är det inte obligatoriskt att utföra en konsekvensbedömning för varje behandling. I stället krävs en konsekvensbedömning endast om en typ av behandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Det faktum att de villkor som utlöser skyldigheten att utföra en konsekvensbedömning inte är uppfyllda innebär emellertid inte någon minskning av personuppgiftsansvarigas generella skyldighet att genomföra åtgärder för att hantera risker för de registrerades rättigheter och friheter på ett lämpligt sätt. I praktiken innebär detta att personuppgiftsansvariga kontinuerligt är skyldiga att bedöma den risk som uppkommer vid deras behandlingar för att identifiera när en typ av behandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

¹⁰ Det ska framhållas att det för hantering av risker i samband med fysiska personers rättigheter och friheter krävs en regelbunden identifiering, analys, uppskattning, utvärdering, behandling (dvs. avhjälpning) och översyn av riskerna. Personuppgiftsansvariga kan inte undgå sitt ansvar genom att täcka riskerna genom försäkringsavtal.

Följande figur illustrerar de grundläggande principerna för konsekvensbedömningen i förordningen:



A. Vad ska en konsekvensbedömning hantera? En enda behandling eller en serie liknande behandlingar.

En konsekvensbedömning kan avse en enda behandling av uppgifter. I artikel 35.1 föreskrivs emellertid att "[e]n enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker". I skäl 92 anges dessutom att "[i]bland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet".

En enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Syftet med konsekvensbedömningarna är att systematiskt studera nya situationer som kan medföra hög risk för fysiska personers rättigheter och friheter, och det föreligger inte något behov av att utföra en konsekvensbedömning i situationer (dvs. behandlingar som utförs i ett särskilt sammanhang och av en särskild anledning) som redan har studerats. Detta kan vara fallet när liknande teknik används för att samla in samma slags uppgifter för samma ändamål. Till exempel kan en grupp kommunala myndigheter som var och en inför ett liknande övervakningssystem utföra en enda konsekvensbedömning som omfattar behandlingen av dessa enskilda personuppgiftsansvariga, eller en järnvägsoperatör (enskild personuppgiftsansvarig) kan täcka videoövervakning i samtliga tågstationer med en konsekvensbedömning. Detta kan även vara tillämpligt på liknande behandlingar som genomförts av olika personuppgiftsansvariga. I dessa fall bör en referenskonsekvensbedömning delas eller göras allmänt tillgänglig. Åtgärder som beskrivs i konsekvensbedömningen ska genomföras och det ska tillhandahållas en motivering varför en enda konsekvensbedömning har utförts.

Om behandlingen omfattar flera personuppgiftsansvariga krävs en exakt definition av deras respektive skyldigheter. Deras konsekvensbedömning ska visa vilken part som är ansvarig för de olika åtgärder som utformats för att behandla risker och för att skydda de registrerades rättigheter och friheter. Varje personuppgiftsansvarig bör uttrycka sina behov och dela användbar information utan att äventyra

hemligheter (t.ex. skydd av affärshemligheter, immateriella rättigheter, konfidentiell affärsinformation) eller avslöja svagheter.

En konsekvensbedömning kan också vara användbar för att bedöma dataskyddets konsekvenser för en teknisk produkt, till exempel maskinvara eller programvara, som sannolikt kommer att användas av olika personuppgiftsansvariga för att utföra olika behandlingar. Den personuppgiftsansvarige som utnyttjar produkten är naturligtvis fortfarande skyldig att utföra sina egna konsekvensbedömningar vad gäller det särskilda genomförandet, men detta kan i förekommande fall göras genom en konsekvensbedömning som upprättats av den som tillhandahållit produkten. Ett exempel kan vara förhållandet mellan en tillverkare av smarta mätare och allmännyttiga företag. Varje tillhandahållare av produkter eller behandlare bör dela användbar information utan att äventyra hemligheter eller att avslöja svagheter så att det uppkommer säkerhetsrisker.

B. Vilka behandlingar är föremål för en konsekvensbedömning? Förutom vid undantag, när de ”sannolikt leder till en hög risk”.

I detta avsnitt beskrivs i vilka situationer en konsekvensbedömning är obligatorisk och när det inte är nödvändigt att genomföra en konsekvensbedömning.

Såvida behandlingen inte omfattas av ett undantag (III.B.a) ska en konsekvensbedömning utföras när behandlingen ”sannolikt leder till en hög risk” (III.B.b).

- a) När är det obligatoriskt med en konsekvensbedömning? När behandlingen ”sannolikt leder till en hög risk”.

Enligt förordningen krävs inte att en konsekvensbedömning utförs för varje behandling som kan leda till en risk för fysiska personers rättigheter och friheter. Att utföra en konsekvensbedömning är obligatoriskt endast om behandlingen ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1, illustrerat av artikel 35.3 och kompletterat av artikel 35.4). Det är särskilt relevant när en ny teknik för databehandling införs¹¹.

I situationer där det är osäkert huruvida en konsekvensbedömning är nödvändig rekommenderar arbetsgruppen att en konsekvensbedömning ändå utförs, eftersom det är ett användbart verktyg för att hjälpa personuppgiftsansvariga att iakttä dataskyddslagstiftningen.

Även om en konsekvensbedömning kan krävas under andra omständigheter finns i artikel 35.3 några exempel på när en behandling ”sannolikt leder till en hög risk”:

- ”a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer¹².

¹¹ Se skälen 89, 91 och artikel 35.1 och 35.3 för ytterligare exempel.

¹² Se skäl 75: ”framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler”.

- b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10¹³.
- c) Systematisk övervakning av en allmän plats i stor omfattning.”

Såsom orden ”framför allt” i första meningen i artikel 35.3 i förordningen antyder är detta inte avsett att vara en uttömmande förteckning. Det kan föreligga ”hög risk” vid behandlingar som inte omfattas av denna förteckning men som ändå medför liknande höga risker. Sådana behandlingar bör också vara föremål för konsekvensbedömningar. Av denna anledning går de kriterier som utvecklas nedan ibland utöver en enkel förklaring av vad som ska förstås med de tre exempel som ges i artikel 35.3 i förordningen.

För att tillhandahålla en mer konkret uppsättning av behandlingar som kräver en konsekvensbedömning på grund av deras inneboende höga risk, med beaktande av de särskilda elementen i artikel 35.1 och 35.3 a–c, den förteckning som ska antas på nationell nivå enligt artikel 35.4 och skälen 71, 75 och 91, och andra hänvisningar i förordningen till behandlingar som ”sannolikt leder till en hög risk”¹⁴ ska följande nio kriterier beaktas.

1. Utvärdering eller poängsättning, inbegripet profilering och förutsägelse, särskilt ”aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar” (skälen 71 och 91). Exempel på detta kan innefatta finansinstitut som granskar sina kunder mot en databas för kreditupplysning eller mot en databas för bekämpning av penningtvätt och finansiering av terrorism, eller ett bioteknikföretag som erbjuder genetiska tester direkt till konsumenter för att bedöma och förutse risker för sjukdomar/hälsorisker, eller ett företag som utvecklar profiler för beteende eller marknadsföring som grundas på användning av eller navigering på dess webbplats.
2. Automatiskt beslutsfattande med rättsliga eller liknande betydande följder: behandling som har i syfte att fatta beslut om registrerade som har ”rättsliga följder för fysiska personer” eller ”på liknande sätt i betydande grad påverkar fysiska personer” (artikel 35.3 a). Till exempel kan behandlingen leda till utestängning eller diskriminering av enskilda. Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium. Ytterligare förklaringar om dessa begrepp kommer att tillhandahållas i arbetsgruppens kommande riktlinjer om profilering.
3. Systematisk övervakning: behandling som används för att observera, övervaka eller kontrollera registrerade, inbegripet uppgifter som har samlats in genom nätverk eller ”[s]ystematisk övervakning av en allmän plats” (artikel 35.3 c)¹⁵. Denna typ av övervakning är

¹³ Se skäl 75: ”om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas”.

¹⁴ Se t.ex. skälen 75, 76, 92 och 116.

¹⁵ Arbetsgruppen tolkar att ”systematisk” innebär att övervakningen har en eller flera av följande kännetecken (se arbetsgruppens riktlinjer om dataskyddsombud 16/EN WP 243):

- Övervakningen sker enligt ett system,
- den har arrangerats i förväg, är organiserad eller metodisk,
- äger rum som en del i en allmän plan för insamling av uppgifter,
- och/eller utförs som en del av en strategi.

ett kriterium eftersom personuppgifter kan samlas in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas. Dessutom kan det vara omöjligt för enskilda att undvika att bli föremål för sådan behandling på allmän plats (eller allmänt tillgängliga platser).

4. Känsliga uppgifter eller uppgifter av mycket personlig karaktär: detta omfattar särskilda kategorier av personuppgifter såsom de definieras i artikel 9 (till exempel information om enskildas politiska åsikter) liksom personuppgifter som gäller fällande domar i brottmål och brott såsom de definieras i artikel 10. Ett exempel kan vara ett allmänt sjukhus som lagrar patienternas journaler eller en privatdetektiv som sparar uppgifter om gärningsmän. Utöver dessa bestämmelser i förordningen kan vissa kategorier av uppgifter anses öka den eventuella risken för enskildas rättigheter och friheter. Sådana personuppgifter anses vara känsliga (såsom detta begrepp normalt förstås), eftersom de är kopplade till verksamhet som har samband med hushållet och privat verksamhet (såsom elektronisk kommunikation vars konfidentialitet ska skyddas), eller eftersom de påverkar utövandet av en grundläggande rättighet (såsom lokaliseringssuppgifter vars insamling medför att den fria rörligheten ifrågasätts) eller eftersom åsidosättandet av dessa rättigheter entydigt får allvarliga konsekvenser för den registrerades dagliga liv (såsom finansiella uppgifter som kan användas för betalningsbedrägeri). I detta avseende kan det ha betydelse om uppgifterna redan har offentliggjorts av den registrerade eller av tredje man. Det faktum att personuppgifterna har offentliggjorts kan beaktas som en faktor vid bedömningen av om uppgifterna förväntades användas vidare för särskilda ändamål. Detta kriterium kan även omfatta uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.
5. Uppgifter som behandlas i stor omfattning: I förordningen definieras inte vad som avses med stor omfattning, även om viss vägledning ges i skäl 91. Arbetsgruppen rekommenderar i vart fall att följande faktorer beaktas särskilt vid bedömningen av huruvida behandlingen utförs i stor omfattning¹⁶:
 - a. Antalet registrerade som berörs, antingen som ett särskilt antal eller som en andel av den aktuella populationen.
 - b. Mängden uppgifter och/eller variationen av hanterade dataelement.
 - c. Databehandlingens varaktighet eller beständighet.
 - d. Behandlingens geografiska omfattning.
6. Matchande eller kombinerande uppgiftsserier, som till exempel kommer från två eller flera behandlingar av uppgifter som utförs i olika syften och/eller av olika personuppgiftsansvariga på ett sätt som överstiger den registrerades rimliga förväntningar¹⁷.
7. Uppgifter som rör sårbara registrerade (skäl 75): behandling av denna typ av uppgifter är ett kriterium på grund av en ökad maktobalans mellan de registrerade och den personuppgiftsansvarige, vilket innebär att det kan vara svårt för enskilda att på ett enkelt sätt lämna samtycke eller motsätta sig behandling av sina uppgifter eller utöva sina rättigheter. Sårbara registrerade kan omfatta barn (de kan anses inte vara i stånd att medvetet och med eftertanke motsätta sig eller lämna samtycke till behandling av sina uppgifter), anställda, mer

Arbetsgruppen anser att ”allmän plats” ska tolkas så att det innebär alla platser som är tillgängliga för allmänheten, till exempel ett torg, ett köpcentrum, en gata, en marknad, en tågstation eller ett offentligt bibliotek.

¹⁶ Se arbetsgruppens riktlinjer 16/EN WP 243 om dataskyddsombud.

¹⁷ Se förklaringen i arbetsgruppens yttrande 13/EN WP 203 om ändamålsbegränsningar, s. 24.

sårbara befolkningsgrupper som behöver socialt skydd (psykiskt sjuka personer, asylsökande, äldre personer, patienter osv.), samt i vart fall situationer där en obalans kan fastställas vad gäller förhållandet mellan den registrerade och den personuppgiftsansvarige.

8. **Innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar**, såsom en kombination av fingeravtryck och ansiktigenkänning för förbättrad fysisk åtkomstkontroll osv. I förordningen klargörs (artikel 35.1 och skälen 89 och 91) att användningen av ny teknik, definierad ”i enlighet med den uppnådda nivån av teknisk kunskap” (skäl 91), kan innebära att det behövs en konsekvensbedömning. Detta beror på att användningen av sådan teknik kan omfatta nya former av insamling och användning av uppgifter, eventuellt med hög risk för enskildas rättigheter och friheter. De personliga och sociala konsekvenserna av användningen av ny teknik kan vara okända. En konsekvensbedömning hjälper den personuppgiftsansvarige att förstå och hantera sådana risker. Till exempel kan vissa ”sakernas internet”-applikationer få betydande konsekvenser för enskildas dagliga liv och integritet och således kräva en konsekvensbedömning.
9. Om behandlingen i sig ”hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal” (artikel 22 och skäl 91). Detta omfattar behandlingar som syftar till att medge, ändra eller neka registrerade tillgång till en tjänst eller att ingå ett avtal. Ett exempel på detta är när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

I de flesta situationer kan en personuppgiftsansvarig anse att en konsekvensbedömning ska utföras om dessa två kriterier är uppfyllda. Generellt sett anser arbetsgruppen att ju fler kriterier behandlingen uppfyller, desto mer sannolikt är det att det föreligger en hög risk för de registrerades rättigheter och friheter, och att det därför krävs en konsekvensbedömning, oberoende av vilka åtgärder som den personuppgiftsansvarige planerar att vidta.

En personuppgiftsansvarig kan emellertid i vissa fall anse att en behandling som endast uppfyller ett av dessa kriterier kräver en konsekvensbedömning.

Följande exempel illustrerar hur kriterierna bör användas för att bedöma huruvida en särskild behandling kräver en konsekvensbedömning.

Exempel på behandling	Eventuella relevanta kriterier	Kommer det sannolikt att krävas en konsekvensbedömning?
Ett sjukhus behandlar patienternas genetiska uppgifter och hälsouppgifter (informationssystem på sjukhus).	<ul style="list-style-type: none"> - <u>Känsliga uppgifter eller uppgifter av mycket personlig karaktär.</u> - Uppgifter som rör sårbara registrerade. - Uppgifter som behandlas i stor omfattning. 	Ja
Användning av ett kamerasystem för att övervaka körbeteendet på motorvägar. Den personuppgiftsansvarige planerar att använda ett system för intelligent videoanalys för att skilja ut bilar och automatiskt känna igen registreringsskyltar.	<ul style="list-style-type: none"> - Systematisk övervakning. - Innovativ användning eller tillämpning av tekniska eller organisatoriska lösningar. 	

Exempel på behandling	Eventuella relevanta kriterier	Kommer det sannolikt att krävas en konsekvensbedömning?
Ett företag övervakar systematiskt sina anställdas aktiviteter, inbegripet övervakning av deras arbetsstation, internetaktivitet osv.	<ul style="list-style-type: none"> - Systematisk övervakning. - Uppgifter som rör sårbara registrerade. 	
Insamling av uppgifter från offentliga sociala medier för generering av profiler.	<ul style="list-style-type: none"> - Utvärdering eller poängsättning. - Uppgifter som behandlas i stor omfattning. - Matchande eller kombinerande uppgiftsserier. - <u>Känsliga uppgifter eller uppgifter av mycket personlig karaktär:</u> 	
Ett institut inrättar en databas för kreditvärdering eller bedrägerier på nationell nivå.	<ul style="list-style-type: none"> - Utvärdering eller poängsättning. - Automatiskt beslutsfattande med rättsliga eller liknande betydande följder. - Hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal. - <u>Känsliga uppgifter eller uppgifter av mycket personlig karaktär:</u> 	
Lagring i arkiveringssyfte av pseudonymiserade känsliga personuppgifter som rör sårbara registrerade från forskningsprojekt eller kliniska provningar.	<ul style="list-style-type: none"> - Känsliga uppgifter. - Uppgifter som rör sårbara registrerade. - Hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal. 	
Behandling av ”personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud” (skäl 91).	<ul style="list-style-type: none"> - <u>Känsliga uppgifter eller uppgifter av mycket personlig karaktär.</u> - Uppgifter som rör sårbara registrerade. 	Nej
En nättidskrift använder en sändlista för att dagligen skicka ett allmänt nyhetsbrev till sina prenumeranter.	<ul style="list-style-type: none"> - Uppgifter som behandlas i stor omfattning. 	
En webbplats för e-handel som visar annonser för begagnade bildelar med begränsad profilering och med utgångspunkt i varor som visats eller köpts på den egna webbplatsen.	<ul style="list-style-type: none"> - Utvärdering eller poängsättning. 	

En behandling kan omvänt överensstämja med ovannämnda situationer, men den personuppgiftsansvarige kan ändå göra bedömningen att den ”sannolikt inte leder till en hög risk”. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs, och inkludera/registrera dataskyddsombudets synpunkter.

Dessutom, som en del av ansvarsprincipen, ska varje personuppgiftsansvarig ”föra ett register över behandling som utförts under dess ansvar”, inbegripet bland annat ändamålen med behandlingen, en beskrivning av kategorierna av uppgifter och mottagarna av uppgifter och ”[o]m möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1” (artikel 30.1), och den personuppgiftsansvarige måste bedöma huruvida en hög risk är sannolik, även om han eller hon till sist beslutar att inte utföra en konsekvensbedömning.

Anmärkning: Tillsynsmyndigheterna är skyldiga att upprätta, offentliggöra och översända en förteckning till Europeiska dataskyddsstyrelsen över de behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd (artikel 35.4)¹⁸. De kriterier som fastställs ovan kan hjälpa tillsynsmyndigheterna att upprätta en sådan förteckning, med mer specifikt innehåll som läggs till efterhand om det är lämpligt. Till exempel kan behandlingen av alla typer av biometriska uppgifter eller uppgifter om barn anses vara relevanta för utvecklingen av en förteckning enligt artikel 35.4.

- b) När krävs det inte en konsekvensbedömning? Om behandlingen inte ”sannolikt leder till en hög risk”, eller det finns en liknande konsekvensbedömning, eller den har godkänts före maj 2018, eller har en rättslig grund, eller finns med i förteckningen över behandlingar som inte kräver en konsekvensbedömning.

Arbetsgruppen anser att det inte krävs en konsekvensbedömning i följande situationer:

- **Om behandlingen inte** ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).
- **Om behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning har utförts.** I sådana situationer kan resultat från konsekvensbedömningar för liknande behandlingar användas (artikel 35.1¹⁹).
- Om behandlingen har kontrollerats av en tillsynsmyndighet före maj 2018 under särskilda villkor som inte har ändrats²⁰ (se III.C).
- **Om en behandling** enligt artikel 6.1 c eller e **har en rättslig grund** i unionsrätten eller i en medlemsstats nationella rätt, om denna lagstiftning reglerar den specifika behandlingsåtgärden **och om en konsekvensbedömning redan har genomförts** som en del av fastställandet av denna rättsliga grund (artikel 35.10)²¹, förutom om en medlemsstat har angett att det är nödvändigt att utföra en konsekvensbedömning före behandlingen.
- **Om behandlingen finns med på den frivilliga förteckning (som fastställts av tillsynsmyndigheten) över behandlingar** för vilka det inte krävs någon

¹⁸ I detta avseende ”ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen” (artikel 35.6).

¹⁹ ”En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.”

²⁰ ”Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.” (Skäl 171.)

²¹ Om en konsekvensbedömning utförs under utarbetandet av den lagstiftning som utgör rättslig grund för behandlingen, krävs det sannolikt en översyn innan den börjar användas, eftersom den lagstiftning som antas kan skilja sig från förslaget på sätt som påverkar integriteten och frågor som rör uppgiftsskydd. Vid den tidpunkt när lagstiftningen antogs fanns kanske inte heller tillräckliga tekniska detaljer avseende den faktiska behandlingen, även om den åtföljdes av en konsekvensbedömning. I sådana fall kan det fortfarande vara nödvändigt att utföra en särskild konsekvensbedömning innan den faktiska behandlingen utförs.

konsekvensbedömning (artikel 35.5). En sådan förteckning kan innehålla behandlingar som uppfyller de villkor som specificeras av myndigheten, i synnerhet genom riktlinjer, särskilda beslut eller tillstånd, bestämmelser för efterlevnad osv. (t.ex. i Frankrike, tillstånd, undantag, förenklade regler, paket för efterlevnad osv.). I sådana situationer, och med förbehåll för en omprövning av den behöriga tillsynsmyndigheten, krävs det inte någon konsekvensbedömning. Detta är endast fallet om behandlingen fullt ut omfattas av det relevanta förfarande som anges i förteckningen och fortsätter att fullt ut uppfylla alla relevanta krav i förordningen.

C. Vad gäller för redan befintliga behandlingar? Konsekvensbedömningar krävs under vissa omständigheter.

Kravet på att utföra en konsekvensbedömning är tillämpligt på befintliga behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter och där riskerna ändrats, med beaktande av behandlingens art, omfattning, sammanhang och ändamål.

Det krävs inte någon konsekvensbedömning för behandlingar som, i enlighet med artikel 20 i direktiv 95/46/EG, har kontrollerats av en tillsynsmyndighet eller dataskyddsbudet och vars genomförande inte har ändrats sedan föregående kontroll. ”Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.” (Skäl 171.)

Omvänt innebär detta att en behandling av uppgifter vars genomförandevillkor (omfattning, ändamål, insamlade personuppgifter, de personuppgiftsansvarigas eller mottagarnas identiteter, lagringstid, tekniska och organisatoriska åtgärder osv.) har ändrats sedan den föregående kontroll som tillsynsmyndigheten eller dataskyddsbudsmannen har genomfört, och som sannolikt leder till en hög risk, bör bli föremål för en konsekvensbedömning.

Dessutom kan en konsekvensbedömning krävas efter en ändring av de risker som uppkommer genom behandlingen²², till exempel för att ny teknik har börjat användas eller för att personuppgifter används för ett annat ändamål. Uppgiftsbehandlingen kan utvecklas snabbt och nya sårbarheter kan uppstå. Det bör därför noteras att en översyn av en konsekvensbedömning inte enbart främjar kontinuerliga förbättringar, utan även är viktig för att bibehålla nivån på uppgiftsskyddet över tid i en föränderlig miljö. En konsekvensbedömning kan också krävas på grund av förändringar i behandlingens organisatoriska eller sociala sammanhang, till exempel för att effekterna av vissa automatiska beslut har ökat i betydelse, eller för att nya kategorier av registrerade blir sårbara för diskriminering. Vart och ett av dessa exempel kan medföra att den risk som uppkommer vid den aktuella behandlingen ändras.

Omvänt kan vissa ändringar också minska risken. Till exempel kan en behandling utvecklas så att besluten inte längre är automatiserade eller att övervakningen inte längre är systematisk. Om detta är fallet kan en översyn av den riskanalys som gjorts visa att det inte längre krävs någon konsekvensbedömning.

Som god praxis **bör en konsekvensbedömning ses över kontinuerligt och omvärderas regelbundet**. Även om det inte krävs en konsekvensbedömning den 25 maj 2018 är det därför

²² Beroende på sammanhanget, insamlade uppgifter, ändamål, funktioner, behandlade personuppgifter, mottagare, uppgiftskombinationer, risker (stödjande tillgångar, riskkällor, eventuell påverkan, hot osv.), säkerhetsåtgärder och internationella överföringar.

nödvändigt för den personuppgiftsansvarige att utföra en sådan konsekvensbedömning, vid lämplig tidpunkt och som en del av dennes allmänna ansvarsskyldigheter.

D. Hur ska en konsekvensbedömning utföras?

- a) Vid vilken tidpunkt ska en konsekvensbedömning utföras? Före behandlingen.

Konsekvensbedömningen ska utföras ”före behandlingen” (artikel 35.1 och 35.10, skälen 90 och 93)²³. Detta är förenligt med principerna om inbyggt dataskydd och dataskydd som standard (artikel 25 och skäl 78). Konsekvensbedömningen bör betraktas som ett verktyg för att underlätta beslutsfattandet avseende behandlingen.

Konsekvensbedömningen bör påbörjas så tidigt som det är praktiskt möjligt vid utformningen av behandlingen, även om vissa delar av behandlingen fortfarande är okända. En uppdatering av konsekvensbedömningen under projektets livscykel säkerställer ett beaktande av uppgiftsskydd och integritet och uppmuntrar skapandet av lösningar som främjar överensstämmelse. Det kan även vara nödvändigt att upprepa enskilda steg av bedömningen allt eftersom utvecklingsprocessen framskrider, eftersom valet av vissa tekniska eller organisatoriska åtgärder kan påverka allvaret i eller sannolikheten för de risker som uppkommer genom behandlingen.

Det faktum att konsekvensbedömningen kan behöva uppdateras när behandlingen väl har påbörjats är inte ett giltigt skäl för att skjuta upp eller underlåta att utföra en konsekvensbedömning. Konsekvensbedömningen är en pågående process, särskilt om behandlingen är dynamisk och föremål för löpande förändringar. **Utförandet av en konsekvensbedömning är en pågående process, inte ett förfarande som vi ett enda tillfälle.**

- b) Vem är skyldig att utföra konsekvensbedömningen? Den personuppgiftsansvarige, tillsammans med dataskyddsombudet och personuppgiftsbiträdena.

Den personuppgiftsansvarige är ansvarig för att säkerställa att konsekvensbedömningen utförs (artikel 35.2). Konsekvensbedömningen kan utföras av någon annan, inom eller utanför organisationen, men den personuppgiftsansvarige har det yttersta ansvaret för denna uppgift.

Den personuppgiftsansvarige ska även rådfråga dataskyddsombudet, om ett sådant har utsetts (artikel 35.2), och dessa råd och de beslut som den personuppgiftsansvarige fattar bör dokumenteras i konsekvensbedömningen. Dataskyddsombudet bör även övervaka genomförandet av konsekvensbedömningen (artikel 39.1 c). Ytterligare vägledning finns i arbetsgruppens riktlinjer 16/EN WP 243 om dataskyddsombud.

Om behandlingen helt eller delvis utförs av ett personuppgiftsbiträde **bör personuppgiftsbiträdet bistå den personuppgiftsansvarige vid utförandet av konsekvensbedömningen** och tillhandahålla nödvändig information (i enlighet med artikel 28.3 f).

Den personuppgiftsansvarige ska ”när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare” (artikel 35.9). Arbetsgruppen anser följande:

²³ Förutom om det redan finns en befintlig behandling som har kontrollerats av tillsynsmyndigheten, i vilket fall en konsekvensbedömning ska utföras innan betydande förändringar genomförs.

- Dessa synpunkter kan inhämtas på olika sätt, beroende på sammanhanget (t.ex. en allmän studie med koppling till behandlingens ändamål och medel, en fråga till företrädarna för personalen eller vanliga enkäter som skickas till den personuppgiftsansvariges framtida kunder) som säkerställer att den personuppgiftsansvarige har en laglig grund för att behandla de personuppgifter som berörs av inhämtningen av sådana synpunkter. Det bör emellertid observeras att ett samtycke till behandling uppenbarligen inte är ett sätt att inhämta synpunkter från de registrerade.
- Om den personuppgiftsansvariges slutliga beslut skiljer sig från de registrerades synpunkter ska de skäl som han eller hon har för att gå vidare eller inte dokumenteras.
- Den personuppgiftsansvarige ska även dokumentera sin motivering för att inte inhämta synpunkter från de registrerade, om han eller hon beslutar att det inte är lämpligt, till exempel om detta skulle äventyra företagets affärsplaner, eller vara oproportionerligt eller ogenomförbart.

Slutligen är det god praxis att definiera och dokumentera andra särskilda roller och skyldigheter, beroende på interna strategier, förfaranden och regler, till exempel följande:

- Om särskilda affärsenheter får föreslå att en konsekvensbedömning ska utföras bör dessa enheter tillhandahålla uppgifter till konsekvensbedömningen och vara involverade i dess valideringsprocess.
- När så är lämpligt rekommenderas att synpunkter inhämtas från oberoende experter från olika yrkesgrupper²⁴ (jurister, it-expert, säkerhetsexperten, sociologer, etikspecialister osv.).
- Personuppgiftsbiträdenas roller och ansvarsområden ska fastställas i ett avtal. Konsekvensbedömningen ska utföras med hjälp av personuppgiftsbiträdet och med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå (artikel 28.3 f).
- Chefen för informationssäkerhet, om en sådan har utsetts, samt dataskyddsombudet, kan föreslå att den personuppgiftsansvarige utför en konsekvensbedömning för en särskild behandling, och bör hjälpa berörda aktörer med avseende på metoden, hjälpa till att utvärdera riskbedömningens kvalitet och huruvida den kvarstående risken är godtagbar, samt utveckla kunskaper som är specifika för personuppgiftsansvariga.
- Informationssäkerhetschefen, om en sådan har utsetts, och/eller it-avdelningen, bör bistå den personuppgiftsansvarige och kan föreslå att en konsekvensbedömning ska utföras avseende en viss behandling, beroende på säkerhetsbehoven eller de operativa behoven.

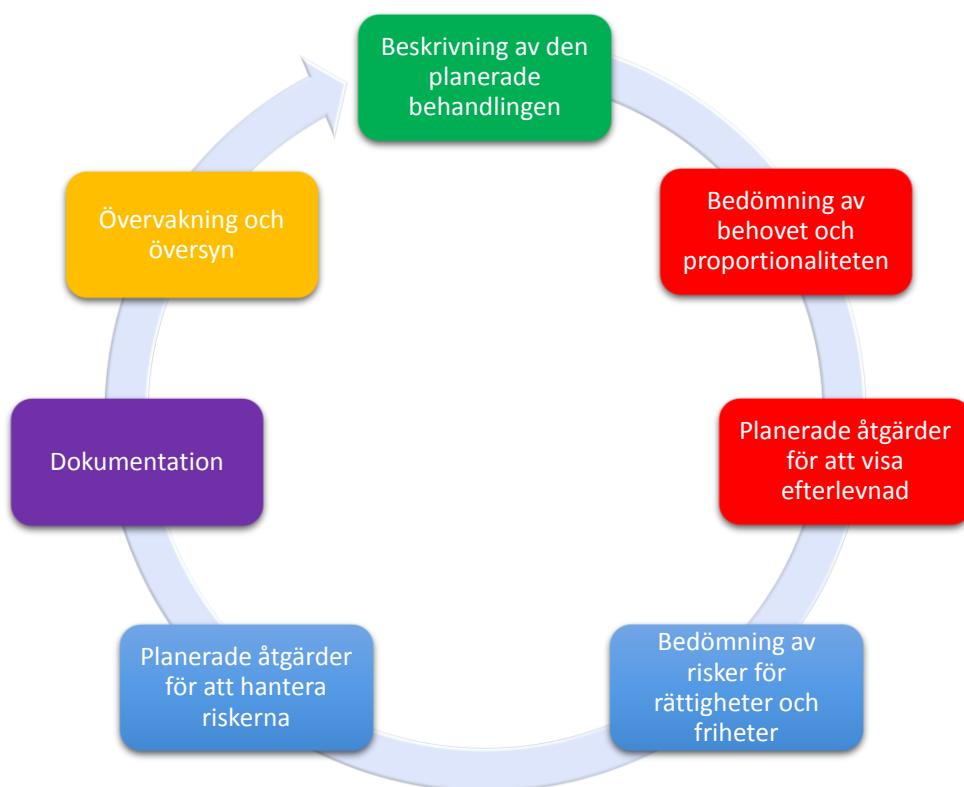
c) Vilken metod ska användas för att utföra en konsekvensbedömning? Olika metoder men gemensamma kriterier.

²⁴ *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf

I förordningen fastställs minimikriterier för en konsekvensbedömning (artikel 35.7 och skälen 84 och 90):

- "[E]n [...] beskrivning av den planerade behandlingen och behandlingens syften",
- "en bedömning av behovet av och proportionaliteten hos behandlingen",
- "en bedömning av [...] [riskerna] för de registrerades rättigheter och friheter",
- "de åtgärder som planeras
 - o för att hantera riskerna",
 - o "för att visa att denna förordning efterlevs".

Följande figur illustrerar det generella återkommande förfarandet för att genomföra en konsekvensbedömning²⁵:



Iakttagande av en uppförandekod (artikel 40) måste beaktas (artikel 35.8) vid bedömningen av konsekvenserna av en databehandling. Detta kan vara användbart för att visa att lämpliga åtgärder har valts eller vidtagits, under förutsättning att uppförandekoden är lämplig för behandlingen. Certifiering, försegling och märkning i syfte att visa att behandlingen av personuppgiftsansvariga och personuppgiftsbiträden är förenlig med förordningen (artikel 42) samt bindande företagsbestämmelser bör också beaktas.

Alla relevanta krav som föreskrivs i förordningen utgör en bred, allmän ram för utformning och genomförande av en konsekvensbedömning. Det praktiska genomförandet av en konsekvensbedömning är beroende av de krav som fastställs i förordningen, vilka kan kompletteras

²⁵ Det bör understrykas att det förfarande som avbildas här är återkommande: i praktiken är det sannolikt att varje steg upprepas flera gånger innan konsekvensbedömningen kan slutföras.

med mer detaljerad praktisk vägledning. Därför är genomförandet av en konsekvensbedömning skalbart. Detta innebär att även mindre registeransvariga kan utforma och genomföra en konsekvensbedömning som är lämplig för deras behandlingar.

I skäl 90 i förordningen fastställs ett antal komponenter från konsekvensbedömningen som överlappar med välkända komponenter för riskhantering (t.ex. ISO 31000²⁶). I fråga om riskhantering är syftet med en konsekvensbedömning att ”hantera risker” för fysiska personers rättigheter och friheter, med hjälp av följande förfaranden, genom

- att fastställa sammanhanget: ”med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken”,
- bedöma riskerna: ”bedöma den höga riskens specifika sannolikhetsgrad och allvar”,
- hantera riskerna: ”minska denna risk” och ”säkerställa personuppgiftsskyddet”, och ”visa att denna förordning efterlevs”.

Anmärkning: Konsekvensbedömningen enligt förordningen är ett verktyg för att hantera riskerna för de registrerade, och således tar den deras perspektiv, såsom är fallet på vissa områden (t.ex. säkerheten i samhället). Omvänt ligger fokus vid riskhantering på andra områden (t.ex. informationssäkerhet) på organisationen.

Enligt förordningen föreskrivs en flexibilitet för personuppgiftsansvariga vad gäller fastställandet av konsekvensbedömningens exakta struktur och form, för att denna ska kunna vara förenlig med befintliga arbetsmetoder. Det finns ett antal olika processer inom EU och globalt som beaktar de komponenter som beskrivs i skäl 90. En konsekvensbedömning ska emellertid – oberoende av form – vara en genuin riskbedömning som gör det möjligt för personuppgiftsansvariga att vidta åtgärder för att hantera riskerna.

Olika metoder (se bilaga 1 för exempel på metoder för uppgiftsskydd och bedömning av konsekvenserna för integriteten) kan användas för att bistå i genomförandet av de grundläggande krav som fastställs i förordningen. För att medge dessa olika tillvägagångssätt och för att personuppgiftsansvariga samtidigt ska kunna iaktta förordningen har gemensamma kriterier identifierats (se bilaga 2). Dessa kriterier klargör de grundläggande kraven i förordningen, men erbjuder tillräckligt utrymme för olika genomförandeformer. Dessa kriterier kan användas för att visa att en viss metod för konsekvensbedömning uppfyller de krav som ställs i förordningen. **Det är upp till den personuppgiftsansvarige att välja en metod, men denna metod bör överensstämma med kriterierna som föreskrivs i bilaga 2.**

Arbetsgruppen uppmuntrar utveckling av sektorspecifika ramverk för konsekvensbedömning. Anledningen är att de kan utnyttja särskilda branschkunskaper, vilket innebär att konsekvensbedömningen kan hantera de särdrag som föreligger vid en viss typ av behandling (t.ex. vissa typer av uppgifter, gemensamma tillgångar, möjliga konsekvenser, hot, åtgärder). Detta innebär att konsekvensbedömningen kan hantera frågor som uppkommer inom en viss ekonomisk sektor, vid användning av viss teknik eller vid genomförande av vissa typer av behandlingar.

²⁶ Riskhanteringsprocesser: kommunikation och samråd, fastställande av sammanhang, riskbedömning, riskbehandling, övervakning och översyn (se termer och definitioner, liksom innehållsförteckning, i förhandsvisningen av ISO 31000: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>).

Slutligen ska ”[d]en personuppgiftsansvarige [...] vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras” (artikel 35.11²⁷).

- d) Är det obligatoriskt att offentliggöra konsekvensbedömningen? Nej, men genom ett offentliggörande av sammanfattningen kan förtroende skapas. Den fullständiga konsekvensbedömningen ska meddelas tillsynsmyndigheten i fall av förhandssamråd eller om dataskyddsmyndigheten så begär.

Det är inte ett rättsligt krav enligt förordningen att offentliggöra en konsekvensbedömning, utan detta är den personuppgiftsansvariges beslut. Personuppgiftsansvariga bör emellertid överväga att åtminstone offentliggöra delar, såsom en sammanfattning eller slutsatserna, av sin konsekvensbedömning.

Syftet med ett sådant förfarande skulle vara att hjälpa till att skapa förtroende för den personuppgiftsansvariges behandlingar, och visa ansvar och transparens. Det är särskilt god praxis att offentliggöra en konsekvensbedömning om behandlingen påverkar allmänheten. Detta kan särskilt vara fallet om en offentlig myndighet utför en konsekvensbedömning.

Den offentliggjorda konsekvensbedömningen behöver inte innehålla hela bedömningen, särskilt om den kan innehålla särskilda uppgifter om säkerhetsrisker för den personuppgiftsansvarige eller röja affärshemligheter eller känslig kommersiell information. Under dessa omständigheter kan den offentliggjorda versionen endast bestå av en sammanfattning av de viktigaste slutsatserna i konsekvensbedömningen, eller till och med endast ett uttalande om att en konsekvensbedömning har genomförts.

Om en konsekvensbedömning avslöjar en hög kvarstående risk är den personuppgiftsansvarige skyldig att samråda med tillsynsmyndigheten före behandlingen (artikel 36.1). Som en del av detta ska konsekvensbedömningen tillhandahållas i sin helhet (artikel 36.3.e). Tillsynsmyndigheten får ge råd²⁸, och kommer inte att äventyra affärshemligheter eller avslöja brister i säkerheten, med förbehåll för de principer som är tillämpliga i varje medlemsstat om allmänhetens tillgång till offentliga handlingar.

E. När ska tillsynsmyndigheten rådfrågas? När den kvarstående risken är hög.

Såsom förklaras ovan

- krävs en konsekvensbedömning om en behandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1; se III.B.a). Som ett exempel anses behandling av hälsouppgifter i stor omfattning sannolikt innebära en hög risk och kräver en konsekvensbedömning.
- Sedan åligger det den personuppgiftsansvarige att bedöma riskerna för de registrerades rättigheter och friheter och att identifiera de planerade åtgärderna²⁹ för att minska dessa risker till en godtagbar nivå och att visa att förordningen efterlevs (artikel 35.7; se III.C.c). Ett exempel kan vara användning av lämpliga tekniska och organisatoriska säkerhetsåtgärder

²⁷ I artikel 35.10 utesluts uttryckligen enbart tillämpning av artikel 35.1–7.

²⁸ Skriftliga råd till den personuppgiftsansvarige behövs bara om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot förordningen enligt artikel 36.2.

²⁹ Inbegripet beaktande av befintlig vägledning från Europeiska dataskyddsstyrelsen och tillsynsmyndigheter och med hänsyn till den senaste utvecklingen och kostnaderna för genomförandet såsom föreskrivs i artikel 35.1.

(effektiv och fullständig diskryptering, robust nyckelhantering, lämplig åtkomstkontroll, säkerställd backup osv.) vid lagring av personuppgifter på bärbara datorer, utöver befintliga strategier (meddelande, samtycke, rätt till åtkomst, rätt till invändning etc.).

I exemplet ovan avseende bärbara datorer kan behandlingen fortsätta utan samråd med tillsynsmyndigheten enligt lydelsen i artikel 36.1 och skälen 84 och 94, om den personuppgiftsansvarige anses ha minskat riskerna tillräckligt. I situationer där den identifierade risken inte kan hanteras på ett tillfredsställande sätt av den personuppgiftsansvarige (dvs. den kvarstående risken fortsatt är hög) ska den personuppgiftsansvarige samråda med tillsynsmyndigheten.

Ett exempel på en oacceptabelt hög kvarstående risk är situationer där de registrerade kan drabbas av betydande eller till och med oåterkalleliga konsekvenser som de inte kan övervinna (t.ex. obehörig åtkomst till uppgifter som innebär risk för de registrerades liv, en uppsägning, en finansiell risk), och/eller när det förefaller uppenbart att risken kommer att inträffa (t.ex. genom att inte kunna minska antalet personer som har tillgång till uppgifterna på grund av delning, användning eller distributionsmetoder, eller om en välkänd sårbarhet inte kan avhjälpas).

När den personuppgiftsansvarige inte kan vidta tillräckliga åtgärder för att minska risken till en godtagbar nivå (dvs. den kvarstående risken är fortfarande hög), krävs samråd med tillsynsmyndigheten³⁰.

Dessutom måste den personuppgiftsansvarige samråda med tillsynsmyndigheten när det i medlemsstatens lagstiftning krävs att personuppgiftsansvariga ska samråda med, och/eller få förhandstillstånd av, tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa (artikel 36.5).

Det bör emellertid påpekas att skyldigheterna att föra ett register över konsekvensbedömningen och vederbörligen uppdatera den kvarstår, oberoende av huruvida det krävs ett samråd med tillsynsmyndigheten på grund av den kvarstående risken.

IV. Slutsatser och rekommendationer

Konsekvensbedömningar är ett användbart sätt för personuppgiftsansvariga att införa databehandlingssystem som överensstämmer med förordningen och kan vara obligatoriska för vissa typer av behandlingar. De är skalbara och kan ha olika former, men i förordningen föreskrivs de grundläggande kraven för en effektiv konsekvensbedömning. Personuppgiftsansvariga bör betrakta utförandet av en konsekvensbedömning som en användbar och positiv åtgärd som stödjer efterlevnaden av lagstiftningen.

I artikel 24.1 fastställs den personuppgiftsansvariges grundläggande ansvar vad gäller efterlevnaden av förordningen. ”Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att

³⁰ Anmärkning: ”pseudonymisering och kryptering av personuppgifter” (samt en minimering av uppgifter, mekanismer för översyn osv.) är inte nödvändigtvis lämpliga åtgärder. De utgör enbart exempel. Vilka åtgärder som är lämpliga beror på sammanhanget och de särskilda riskerna med behandlingen.

säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.”

Konsekvensbedömningen är en grundläggande del av efterlevnaden av förordningen om en behandling av uppgifter med hög risk planeras eller äger rum. Detta innebär att personuppgiftsansvariga bör använda de kriterier som föreskrivs i detta dokument för att fastställa huruvida en konsekvensbedömning måste utföras eller inte. Interna strategier för personuppgiftsansvariga kan medföra att denna förteckning utvidgas utöver de rättsliga kraven i förordningen. Detta bör leda till större förtroende och tillit från registrerade och andra personuppgiftsansvariga.

Om en behandling planeras som sannolikt medför hög risk ska den personuppgiftsansvarige

- välja en konsekvensbedömningsmetod (exempel ges i bilaga 1) som uppfyller kriterierna i bilaga 2, eller specificera och genomföra ett systematiskt förfarande för konsekvensbedömning som
 - o är förenligt med kriterierna i bilaga 2,
 - o integreras med befintliga processer för utformning, utveckling, ändring, risk och operativ översyn i enlighet med interna processer och sammanhang och intern kultur,
 - o involverar berörda parter och tydligt fastställer deras ansvarsområden (personuppgiftsansvarig, dataskyddsombud, registrerade eller deras företrädare, affärsverksamhet, tekniska tjänster, personuppgiftsbiträden och ansvarig för informationssäkerhet osv.);
- tillhandahålla konsekvensbedömningen till den behöriga tillsynsmyndigheten, när det föreligger en sådan skyldighet,
- samråda med tillsynsmyndigheten, om denne har misslyckats med att fastställa tillräckliga åtgärder för att minska den höga risken,
- regelbundet se över konsekvensbedömningen och den behandling som den avser, åtminstone om den risk som behandlingen medför ändras,
- dokumentera de beslut som fattas.

Bilaga 1 – Exempel på befintliga ramverk för konsekvensbedömning i EU

I förordningen specificeras inte vilket förfarande för konsekvensbedömning som ska följas utan i stället får personuppgiftsansvariga införa ett ramverk som kompletterar deras befintliga arbetspraxis, under förutsättning att de komponenter som beskrivs i artikel 35.7 beaktas. Ett sådant ramverk kan vara skraddarsytt för den personuppgiftsansvarige eller gemensamt inom en viss bransch. Tidigare offentliggjorda ramverk som utvecklats av EU:s dataskyddsmyndigheter och branschspecifika ramverk omfattar (men är inte begränsade till) följande:

Exempel på allmänna ramverk inom EU:

- DE: Standard Data Protection Model, V.1.0 – testversion, 2016³¹.
https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
<https://www.cnil.fr/fr/node/15798>
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Exempel på branschspecifika ramverk:

- Konsekvensbedömning av integritets- och uppgiftsskydd för tillämpningar som stöds av radiofrekvensidentifiering (RFID)³².
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Mall för konsekvensbedömning avseende uppgiftsskydd för smarta nät och mätarsystem³³.
http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

En internationell standard kommer också att ge vägledning för de metoder som används vid utförandet av en konsekvensbedömning (ISO/IEC 29134³⁴).

³¹ Enhålligt antagen (med reservation från Bayern) vid den 92:a konferensen för oberoende dataskyddsmyndigheter i förbundsstaten och delstaterna i Kuhlungsborn den 9–10 november 2016.

³² Se även:

- Kommissionens rekommendation av den 12 maj 2009 om genomförandet av principerna om integritets- och dataskydd i tillämpningar som stöds av radiofrekvensidentifiering.
<https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles>
- Yttrande nr 9/2011 om branschens omarbetade förslag till ram för konsekvensbedömning av integritets- och uppgiftsskydd för tillämpningar som stöds av radiofrekvensidentifiering (RFID).
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_sv.pdf

³³ Se även yttrande 7/2013 om mallen för konsekvensbedömning av uppgiftsskydd för smarta nät och mätarsystem (nedan kallad *mallen för konsekvensbedömning av uppgiftsskydd*) som tagits fram av expertgrupp 2 i kommissionens arbetsgrupp för smarta nätverk. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_sv.pdf

Bilaga 2 – Kriterier för en godtagbar konsekvensbedömning

Arbetsgruppen föreslår följande kriterier som kan användas av personuppgiftsansvariga för att bedöma huruvida en konsekvensbedömning, eller en metod för att utföra en konsekvensbedömning, är tillräckligt omfattande för att iakttä förordningen:

- ☐ En systematisk beskrivning av behandlingen tillhandahålls (artikel 35.7 a):
 - ☐ Behandlingens art, omfattning, sammanhang och ändamål beaktas (skäl 90).
 - ☐ Registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer att lagras.
 - ☐ En funktionell beskrivning av behandlingen tillhandahålls.
 - ☐ De tillgångar som är nödvändiga för personuppgifterna (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper) är identifierade.
 - ☐ Efterlevnad av godkända uppförandekoder beaktas (artikel 35.8).
- ☐ En bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b):
 - ☐ De planerade åtgärderna för att visa att förordningen efterlevs har fastställts (artikel 35.7 d och skäl 90), med beaktande av följande:
 - ☐ Åtgärder som bidrar till att behandlingen är proportionell och nödvändig på grundval av
 - ☐ särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),
 - ☐ laglig behandling (artikel 6),
 - ☐ adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
 - ☐ begränsad lagringstid (artikel 5.1 e).
 - ☐ Åtgärder som stärker de registrerades rättigheter:
 - ☐ Information till den registrerade (artiklarna 12, 13 och 14).
 - ☐ Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20).
 - ☐ Rätt till rättelse och radering (artiklarna 16, 17 och 19).
 - ☐ Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
 - ☐ Förhållandet till personuppgiftsbiträden (artikel 28).
 - ☐ Skyddsåtgärder för internationella överföringar (kapitel V).
 - ☐ Förhandssamråd (artikel 36).
- ☐ Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c):
 - ☐ Uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84) eller, mer specifikt, för varje risk (obehörig åtkomst, oönskad ändring och att uppgifter försvinner) ur de registrerades perspektiv:
 - ☐ Beaktande av riskens ursprung (skäl 90).
 - ☐ Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
 - ☐ Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
 - ☐ Uppskattning av sannolikhetsgrad och allvar (skäl 90).
 - ☐ Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).
- ☐ Medverkan från berörda parter:
 - ☐ Rådfrågan av dataskyddsombudet (artikel 35.2).
 - ☐ När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

³⁴ ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Internationella standardiseringsorganisationen (ISO).