

Svar på remiss gällande förslag till: **Föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning, Diarienummer MCF 2026-04554**

Svarande organisation: **Utbetalningsmyndigheten**

Intern referens: **Helena Thofelt**

För generella kommentarer välj "Generellt" under kolumn Kapitel.  
 För kommentarer som gäller allmänna råd välj "Allmänna råd" under kolumn annars välj det kapitel du vill lämna synpunkter på.  
 Välj i kolumn Paragraf vilken paragraf du vill lämna synpunkt på  
 Välj i kolumn Punkt vilken punkt i paragrafen dina kommentarer avser både om de avser paragraf eller allmänt råd.

Synpunkter på konsekvensutredningen lämnas på fylken Konsekvensutredningen

Vänligen skicka dina svar i excelformat för att underlätta sammanställningen av synpunkter.

Synpunkter föreskrifter och allmänna råd					
Kapitel	§	Punkt	Synpunkt	Förslag till ändring	Kommentar
Generellt		Välj	<p>Detaljnivån på styrningen går inte i linje med att uppnå en hög gemensam miniminivå för cybersäkerhet. Det anges i konsekvensutredningen att ledning för hur krav på säkerhetsåtgärder ska konkretiseras kan hämtas från EU-kommissionens genomförandeförordning. Vi anser att föreskrifterna inte omhändertar de krav som finns i genomförandeförordningen. En stor del av de kraven ligger istället som rekommendationer i allmänna råd, vilket leder till en valfrihet hos verksamhetsutövarna som motverkar syftet med att uppnå en gemensam miniminivå.</p> <p>Exempel på dessa områden framgår i synpunkter på konsekvensutredningen.</p>	Omhänderta kraven på säkerhetsåtgärder och utbildning från genomförandeförordningen i föreskriften, så att kraven blir tvingande.	
Generellt		Välj	<p>Generellt innehåller föreskriften väldigt mycket allmänna råd, vilket lämnar utrymme för tolkningar och svårigheter för verksamhetsutövare att veta vilka krav som faktiskt gäller. Det är positivt med utrymme för ett riskbaserat arbetssätt, men vi bedömer att balansen mellan styrning och allmänna råd lämnar för mycket öppet för tolkning i det nya förslaget till föreskrift.</p> <p>Föreskriften är dessutom inkonsekvent skriven mellan olika områden, där vissa detaljeras väldigt mycket, medan andra nästan enbart har allmänna råd.</p>	Se över de allmänna råden och omvandla delar till faktisk styrning (se exempel på områden nedan och under synpunkter på konsekvensutredningen).	
Generellt		Välj	<p>Myndighetens synpunkt från den tidigare remissen kvarstår avseende att den samlade mängden föreskrifter som offentlig förvaltning behöver förhålla sig till avseende informationssäkerhet och cybersäkerhet är inte helt enhetlig när det gäller språkbruk och begrepps användning. Oenhetlighet riskerar att resultera i tolkningssvårigheter för dem som omfattas av flera föreskrifter inom samma område.</p> <p>Dessutom är det en viss inkonsekvens mellan vad som är styrning och allmänna råd mellan den samlade mängden föreskrifter för statliga myndigheter.</p> <p>Exempelvis denna föreskrifts relation till MSBFS 2020:6 och 2020:7.</p>	<p>Säkerställ att föreskrifter som berör informations-/cybersäkerhet för statliga myndigheter använder ett enhetligt språkbruk och etablera en gemensam termbank för föreskrifter som relaterar till samma område.</p> <p>Säkerställ enhetlighet mellan styrning och allmänna råd i föreskrifter som reglerar samma område.</p>	
kap. 1	Välj	Välj	Eftersom begreppet allriskperspektiv är centralt, bör föreskriften förebygga risken för feltolkningar.	Inkludera allrisk-definitionen i ordförklaringskapitlet.	

kap. 3	3	Välj	Förhållandet mellan styrning och allmänna råd ger för stort utrymme för tolkning då allmänna råden är mer omfattande än själva styrningen.		
kap. 3	5	Välj	Det borde vara upp till verksamhetsutövaren att välja roller i den interna organisationen. Så som det är formulerat kan tolkas som styrning, även om det enligt konsekvensutredningens avsnitt 7.2.3.1 framgår att begreppen endast är av författningstekniska skäl.	Skriv om: Verksamhetsutövaren ska utse ansvar för samordning av cybersäkerhet, ansvar för säkerheten i informationsbehandling i system, ansvarig för säkerheten i system.  Flytta förslag på utpekade roller (informationsägare, systemägare, samordnare) till allmänna råd.	
kap. 3	5	Välj	Vi saknar styrning för informationsbehandling som sker utanför system.		
kap. 3	6	Välj	Samordnarens mandat och befogenhet bedöms inte vara tillräckligt tydligt. Vad betyder skrivningen "befogenhet att samordna" i praktiken? För att nå effekt bör samordnarrollen vara en oberoende funktion.	Definiera tydligare vad samordning innebär.	
kap. 3	7	Välj	Styrningen i det här fallet anses vara alltför detaljerad, eftersom den styr arbetssätt mellan informationsägare och systemägare.	Lägg skrivningarna som allmänna råd till 3 kap § 5.	
kap. 3	12	Välj	Otydlig vad som särskiljer dessa riskanalyser: Verksamhetsutövaren ska värdera risker inför utkontraktering av informationsbehandling samt risker med avtal och överenskommelser om förvärv och utkontraktering som innehåller otillräckliga krav på cybersäkerhet. Verksamhetsutövaren ska även värdera risker för sina digitala leveranskedjor.	Skriv om så att det blir tydligt vad som avses med styrningen och tydliggör skillnaden på riskanalys i avtal och överenskommelser om förvärv och utkontraktering i förhållande till risker i de digitala leveranskedjorna.	
kap. 3	12	Välj	Vi saknar delar som genomförandeförordningen anger, exempelvis att följa en riskhanteringsmetod, fastställa risktoleransnivå och kriterier för riskacceptans.	Utöka styrningen med dessa områden.	
kap. 3	13	Välj	Det hänvisas till att säkerhetsåtgärder ska utgå från fastställda kriterier för riskacceptans, men det finns ingen styrning kring att kriterier för riskacceptans ska fastställas i föreskriften.	Se rad 26	
kap. 4	1	Välj	Förvärv av system och utkontraktering av informationsbehandling är större än bara de tekniska aspekterna. Det borde finnas motsvarande område under 3 kap organisatoriska säkerhetsåtgärder.		
kap. 4	1	Välj	Skrivningen om att avtal och överenskommelser som ingåtts före 1 oktober 2026 ska gås igenom anses vara väldigt detaljerad för en föreskrift.	Skrivningen föreslås flyttas till kap 1 tillämpningsområde.	
kap. 4	3	Välj	Förvärv, utkontraktering och digitala leveranskedjor är centralt och styrningen bör framgå i föreskrift och inte vara rekommendationer som allmänna råd.		
kap. 4	4	Välj	Här detaljeras styrningen på ett annat sätt än i föregående paragraf, vilket innebär en inkonsekvens. Styrningen bör läggas på samma nivå genom föreskriften.		
kap. 4	8	Välj	Styrningen är otydlig och öppen för tolkning. De allmänna råden bör omvandlas till styrning och inte vara rekommendationer.		
kap. 4	12	Välj	Otydlig logik kring vad som är styrning och vad som lagts som allmänna råd. T.ex. att följande är ett allmänt råd: säkerställa att autentiseringsuppgifter har tillräcklig längd och komplexitet.		
kap. 4	26	Välj	Att följa leverantörens rekommendationer och relevanta standarder borde vara styrande, inte allmänt råd.		







Svar på remiss gällande förslag till:

Konsekvensutredning för föreskrifter och allmänna om säkerhetsåtgärder och utbildning, Diarienummer MCF 2026-04554

Svarande organisation:

Utbetalningsmyndigheten

Intern referens:

Helena Thofelt

Här kan du lämna synpunkter på konsekvensutredningen.

Synpunkter på föreskrifter lämnas på fliken Föreskrifter

Vänligen skicka dina svar i excelformat för att underlätta

Synpunkter Konsekvensutredningen		
Rubrik, stycke	Synpunkter	Kommentar
	Detaljnivån på styrningen i föreskriften går inte i linje med att uppnå en hög gemensam miniminivå för cybersäkerhet.	Det anges i konsekvensutredningen att ledning för hur krav på säkerhetsåtgärder ska konkretiseras kan hämtas från EU-kommissionens genomförandeförordning. Nedanstående sammanställning visar vilka kapitel och paragrafer i föreskriften (anges som tex 2 kap. 1§ ) som inte fullt ut omhändertar de säkerhetsåtgärder och krav på utbildning som anges i genomförandeförordningen. Styrningen i föreskriften är på en mer övergripande nivå eller så anges styrningen i genomförandeförordningen som ett allmänt råd i föreskriften. När kraven inte är tvingande i styrningen lämnas mycket över till verksamhetsutövarna att själva välja vilken nivå av cybersäkerhet de vill införa och upprätthålla, vilket inte går i linje med NIS2-direktivets och cybersäkerhetslagens syfte - att uppnå en miniminivå av cybersäkerhet inom EU.  Kommentarerna är hämtade från den sammanfattning (rubrik <i>Sammanfattningsvis</i> ) som finns i respektive stycke i konsekvensutredningen.
7.1.1 Ledningens utbildning om säkerhetsåtgärder (2 kap. 1§)		Kraven bedöms ligga i linje med genomförandeförordningen. Genom att de mer detaljerade kraven utgör allmänna råd och därmed är bör-krav ges verksamhetsutövaren flexibilitet avseende utformningen
7.2.2 Interna regler och arbetssätt (3 kap. 3§)		Flera av genomförandeförordningens krav finns i föreskrifterna endast som allmänna råd – dvs rekommendationer inte uttryckliga krav. I dessa delar ger föreskrifterna verksamhetsutövarna mer handlingsfrihet än genomförandeförordningen.
7.2.3 Roller, ansvarsområden och befogenheter (3 kap. 4-8 §§)		De krav som ställs i föreskrifterna rörande ledningens uppgifter bedöms vara mer begränsade än genomförandeförordningens krav på ledningen. Genomförandeförordningen innehåller en rad krav som inte ställs i föreskrifterna exempelvis gällande separation av roller.
7.2.4 Personalsäkerhet (3 kap. 9§)		Föreskrifternas krav bedöms vara på en mer övergripande nivå än genomförandeförordningens motsvarande krav. I delar är genomförandeförordningen förhållandevis detaljerad och reglerar även fler aspekter än föreskrifterna.
7.2.6 Informationsklassning (3 kap.11§)		Genomförandeförordningens krav på klassificering av tillgångar bedöms som något mer omfattande och detaljerade än motsvarande krav i föreskrifterna.
7.2.8 Kontinuitetshantering (3 kap. 14§)		Föreskriftskraven ligger i linje med krav i genomförandeförordningen. I delar är genomförandeförordningens krav mer detaljerade.
7.2.9 Incidenthantering (3 kap. 15§)		Föreskrifterna och genomförandeförordningen reglerar samma områden, det vill säga upptäcka, analysera, begränsa, återhämta sig från och lära av incidenter, men kraven i genomförandeförordningen är betydligt mer detaljerade.
7.2.10 Krishantering (3 kap. 16§)		Föreskriftskraven ligger i linje med motsvarande krav i genomförandeförordningen. I delar är genomförandeförordningens krav mer detaljerade.
7.2.11 Uppföljning och utvärdering (3 kap. 17§)		Föreskrifternas krav skulle kunna beskrivas som en kombination av p.2.2, p.2.3 och p.7 i genomförandeförordningen men är utformade på en mer övergripande nivå som ger verksamhetsutövaren mer utrymme att själva utforma sitt arbete med att följa upp och utvärdera säkerhetsåtgärder.
7.3.1 Förvärv av system och utkontraktering av informationsbehandling (4 kap. 1-3 §§)		Föreskrifternas krav på att utvärdera leverantörer innan förvärv och utkontraktering ställs även i genomförandeförordningen men med ytterligare detaljeringsgrad. Enligt de allmänna råden bör verksamhetsutövaren säkerställa att avtal eller överenskommelser reglerar vissa aspekter. I genomförandeförordningen är ungefär samma krav obligatoriska. Sammanfattningsvis reglerar inte föreskrifterna mer än genomförandeförordningen. Däremot är föreskriftskraven på en mer övergripande nivå och lämnar över mer till verksamhetsutövaren att själv utforma än vad genomförandeförordningen gör.
7.3.2 Utveckling, underhåll och avveckling av system (4 kap. 4-6§§)		Föreskrifternas och genomförandeförordningens krav är lite olika utformade. I delar är dock genomförandeförordningens krav mer detaljerade och tekniska, exempelvis med regler för säker utveckling med bland annat krav på säker kodning och hantering av testdata.
7.3.3 Driftrelaterad dokumentation (4 kap. 7-9§§)		Föreskrifternas krav motsvarar ungefär genomförandeförordningens krav på inventering och förteckning. De allmänna råden konkretiserar visserligen delvis innehållet på en större detaljnivå än i genomförandeförordningen. I och med att det handlar om bör-krav torde dock inte den ökade detaljnivån utgöra någon större ytterligare börda för berörda verksamhetsutövare.
7.3.4 Segmentering (4 kap. 10-11 §§)		Föreskrifterna ställer mer begränsade krav på segmentering än genomförandeförordningen. Flera av de krav som ställs i genomförandeförordningen finns dock i föreskrifterna som allmänna råd som bör-krav.







Kapitel	§	punkt
Välj	Välj	Välj
Generellt	1	Allmänna råd
kap. 1	2	1
kap. 2	3	2
kap. 3	4	3
kap. 4	5	4
kap. 5	6	5
kap. 6	7	6
kap. 7	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	