Diarienummer:
IMY-2025-7052

Datum:
2025-09-01

Nationell rapport till EDPB – analys av genomförande av rätten till radering enligt dataskyddsförordningen

Om detta dokument

Frågorna i detta dokument har i huvudsak utarbetats gemensamt av Europeiska dataskyddsstyrelsens (EDPB) sekretariat och de tillsynsmyndigheter som deltar i EDPB:s samordnade åtgärd år 2025 gällande genomförande av rätten till radering.

Svaren i rapporten kommer att översättas till engelska och lämnas in till EDPB för gemensam analys. Svaren baseras på en analys av de svar som inkommit på IMY:s begäran om information inom ramen för IMY:s genomförande av sin del av åtgärden (dnr IMY 2025-7052, aktbilaga 25-38 och 40-44, inklusive underbilagor). Dokumentets syfte är att underlätta IMY:s interna beredning av denna rapportering till EDPB.

EDPB:s slutliga rapport kommer att publiceras i en rapport i början av nästa år, med IMY:s och övriga deltagande tillsynsmyndigheters svar på engelska som bilaga.

EDPB:s frågor

0. Vad är er tillsynsmyndighets namn?
Integritetsskyddsmyndigheten (IMY)

Inledning

1. Vilket tillvägagångsätt använde ni för genomförandet av er åtgärd?
☐ a. Faktainsamling
☒ b. Faktainsamling + fastställande av uppföljningsåtgärder på grundval av resultaten
☐ c. Ny formell granskning[1]
☐ d. Pågående granskning

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

[1] Användning av tillsynsmyndigheternas formella utredningsbefogenheter för att avgöra om en överträdelse har ägt rum.

2. Om er åtgärd är inriktad på ”Faktainsamling” (dvs. de två första svaren i föregående fråga), besvara följande:

2.a. Identifierade ni tydligt de svarande personuppgiftsansvariga (i motsats till att få anonyma svar)?
☒ Ja
☐ Delvis
☐ Nej

2.b. Planerar ni att inleda formella granskningar om rätten till radering inom en snar framtid till följd av resultaten av faktainsamlingen? Om ja, ange närmare uppgifter om sådana finns tillgängliga.
Nej.

2.c. Om nej, kommer denna faktainsamling att påverka era tillsynsaktiviteter och i så fall hur?
Resultatet av denna faktainsamling kommer att beaktas inom ramen för IMY:s årliga tillsynsplanering för år 2026.

3. För alla tillsynsmyndigheter: Använde ni samma frågeformulär för alla personuppgiftsansvariga, eller använde ni olika frågeformulärversioner för olika typer av personuppgiftsansvariga? Om olika, ange skillnaderna.
Samma frågeformulär användes för alla personuppgiftsansvariga.

4. För alla tillsynsmyndigheter: Ange i förekommande fall a) vilka frågor i det gemensamma frågeformuläret som ni inte tog med i er version av frågeformuläret, b) i vilka frågor ni har ändrat formuleringen i det gemensamma frågeformuläret – ange den ändrade formulering som används per fråga.
I princip användes alla frågorna i det gemensamma frågeformuläret. Dock ändrade vi två av frågorna gällande fallbeskrivningar (fråga 3.4 och 3.8), på så sätt att ingen detaljerad beskrivning av fall som de svarande stött på och den analys som då gjordes behövde lämnas in. Slutligen formulerades fråga 2.1 på så sätt att det var obligatoriskt för respondenten att lämna in sådana upprättade dokument och processbeskrivningar.

5. Har ni andra allmänna kommentarer eller anmärkningar som ni vill framföra (t.ex. när det gäller er användning av frågeformuläret, det valda tillvägagångssättet, särdragen i er åtgärd, osv.)?
Nej.

Del I – Information om de personuppgiftsansvariga som behandlas

6. Hur många personuppgiftsansvariga kontaktade ni?
20

7. Hur många av de kontaktade personuppgiftsansvariga svarade? Observera att vi ber er att lämna alla följande svar baserat på antalet personuppgiftsansvariga som faktiskt svarade på enkäten/era frågor.
20

8. Om det finns en lucka mellan svaren på de två frågorna ovan, har ni identifierat den eller de främsta orsakerna till luckan?
Inte tillämpligt.

9. Ange de svarande personuppgiftsansvarigas verksamhetsområden. Ange hur många (motsvarande) personuppgiftsansvariga som respektive alternativ är tillämpligt på. (Fråga 1.2 i frågeformuläret)

a. Offentlig sektor	7
b. Privat sektor	13
c. Annat (om så, ange vad)	0

10. Ange inom vilken sektor (kärnverksamhet) de svarande personuppgiftsansvariga huvudsakligen är verksamma inom. (Fråga 1.3, 1.3.1 i frågeformuläret)

a. Utbildning	0
b. Hälso- och sjukvård	5
c. Social omsorg	0
d. Försäkring	2
e. Finans	2
f. it	1
g. Detaljhandel	1
h. Logistik	0
i. Kollektivtrafik	3
j. Telekommunikation	2
k. Posttjänster	0
l. Reklam	0
m. Marknadsföringstjänster	0
n. Underhållning	1
o. Information/journalistik	1
p. Vetenskaplig/historisk forskning	0
q. Kreditvärdering	0

r. Leverantör av infrastruktur/samhällsnyttig tjänst (t.ex. energi)	0
s. Bygg och bostad	0
t. Tillverkning	0
u. Konsultverksamhet	0
v. Offentlig förvaltning	4
w. Annat (om så, specificera)	1 Regional utveckling och kultur

11. Ange vilken kategori[2] de svarande personuppgiftsansvariga tillhör. (Fråga 1.4, 1.4.1 i frågeformuläret)

a. Mikroföretag	0
b. Småföretag	0
c. Medelstort företag	1
d. Stort företag	12
e. Ideell organisation	0
f. Statlig myndighet	3
g. Kommunal/regional myndighet	3
h. Administrativ myndighet/organ/kontor (t.ex. arbetsförmedling)	0
i. Skola/universitet/utbildningsanstalt	0
j. Annat (om så, specificera)	1 Regionalt ägt aktiebolag (bolag ägt av det allmänna)

12.a. Vilken kategori av registrerade berörs <u>främst</u> av de svarande personuppgiftsansvarigas behandling? (Fråga 1.5, 1.5.1 i frågeformuläret)

a. Potentiella kunder	0
b. Kunder	13
c. Entreprenörer	0

[2] Upplysning: Information om företagskategorierna finns på https://single-market-economy.ec.europa.eu/smes/sme-definition_en?prefLang=se.

d. Arbetssökande	0
e. Anställda	0
f. Sökande (av allmännyttiga tjänster)	0
g. Medborgare (för den offentliga sektorn)	4
h. Patienter	3
i. Annat (specificera)	0

12.b. Enligt de svarande personuppgiftsansvariga är av dessa registrerade även: (Fråga 1.5.2 i frågeformuläret)

a. Barn	14
b. Utsatta personer (t.ex. äldre, asylsökande, etniska minoriteter, personer med funktionsnedsättning)	13
c. Ej tillämpligt	5

13. Ange ett ungefärligt antal av alla registrerade som berörs av de svarande personuppgiftsansvarigas behandling: (Fråga 1.6 i frågeformuläret)

a. Färre än 100	0
b. 101–1 000	0
c. 1 001–10 000	0
d. 10 001–100 000	0
e. 100 001–500 000	1
f. 500 001–1 000 000	0
g. Fler än 1 000 000	19

14. Vilka typer av personuppgifter berörs främst av de svarande personuppgiftsansvarigas behandling? (Fråga 1.7, 1.7.1, 1.7.2 i frågeformuläret)

a. Kontaktuppgifter	19
b. Betalningsuppgifter	12
c. Identifieringsuppgifter	17

d. Marknadsföringsuppgifter	7
e. Känsliga uppgifter i den mening som avses i artikel 9 i dataskyddsförordningen, t.ex. uppgifter om hälsa, sexualliv eller sexuell läggning, ras eller etniskt ursprung, politiska åsikter, religiös övertygelse, biometriska och genetiska uppgifter	11
f. Uppgifter av mycket personlig karaktär i den mening som avses i artikel 10 i dataskyddsförordningen, t.ex. uppgifter om fällande domar i brottmål och lagöverträdelser som innefattar brott	2
g. Annat (om så, specificera)	2 T.ex. trafikuppgifter, lokaliseringsuppgifter och internetåtkomstuppgifter. 1 Uppgifter om kundernas försäkringsavtal, de försäkrade objekten, skadan och skadehändelse. 1 Användardata såsom lyssningshistorik.

15.a. För fråga 1.8 i frågeformuläret för personuppgiftsansvariga, för hur många år bad ni personuppgiftsansvariga att tillhandahålla siffror (välj ett):
☒ 1 år ☐ 3 år ☐ Annat (om så, specificera): Inte tillämpligt.

15.b. Hur många begäranden om radering i enlighet med artikel 17 i dataskyddsförordningen mottog de svarande personuppgiftsansvariga under den tidsram som anges nedan (ungefär)? (Fråga 1.8 i frågeformuläret)
Ange antalet svarande personuppgiftsansvariga på de relevanta raderna baserat på de siffror som ni samlade in (t.ex. mottog tio svarande mellan 11 och 50 begäranden 2023 men 0 under 2024). Som en påminnelse bör siffror lämnas åtminstone för 2024 (och för 2023, om siffrorna för 2024 är lika med 0, och 2022 om siffrorna för 2024 och 2023 är lika med 0). Ange också när siffrorna är lika med 0.

	2024*	**2023**	**2022**
0	1	Inte tillämpligt.	Inte tillämpligt.
1–10	5	Inte tillämpligt.	Inte tillämpligt.
11–50	4	Inte tillämpligt.	Inte tillämpligt.

51–100	2	Inte tillämpligt.	Inte tillämpligt.
101–500	2	Inte tillämpligt.	Inte tillämpligt.
mer än 500	6	Inte tillämpligt.	Inte tillämpligt.

15.c. För de tillsynsmyndigheter som begärde siffror för flera år, kan ni fylla i denna tabell? (Vi är särskilt intresserade av att veta om de svarande personuppgiftsansvariga som rapporterade att de hade mottagit 0 begäran under 2024 också hade samma antal föregående år.)

	2024*	**2024-2023**	**2024-2022**
0	Inte tillämpligt.	Inte tillämpligt.	Inte tillämpligt.

15.d. Ange antal personuppgiftsansvariga som inte lämnade några siffror för denna fråga (men som svarade på frågeformuläret och de andra frågorna).
0

16.a. För fråga 1.9 i frågeformuläret för personuppgiftsansvariga, för hur många år bad ni personuppgiftsansvariga att tillhandahålla siffror (välj ett):
☒ 1 år ☐ 3 år ☐ Annat (om så, specificera): Inte tillämpligt.

16.b. Av dessa begäranden, hur stor andel var andelen begäranden som de svarande personuppgiftsansvariga avslog (ungefär)? Ange antalet svarande personuppgiftsansvariga på de relevanta raderna baserat på de siffror som ni samlade in (t.ex. tio svarande personuppgiftsansvariga avslog 40 % av begärandena 2023 men 0 % 2024).

	2024*	**2023**	**2022**
0%	4	Inte tillämpligt.	Inte tillämpligt.
10%	6	Inte tillämpligt.	Inte tillämpligt.
20%	1	Inte tillämpligt.	Inte tillämpligt.
30%	0	Inte tillämpligt.	Inte tillämpligt.
40%	1	Inte tillämpligt.	Inte tillämpligt.
mer än 50 %	7	Inte tillämpligt.	Inte tillämpligt.

16.c. För de tillsynsmyndigheter som genomfört en granskning, är ert intryck att de svarande personuppgiftsansvarigas avslag på begäranden överlag varit motiverade?
☐ Ja ☐ Nej (om så, förklara skälen, t.ex. att svarande personuppgiftsansvariga har avslagit alltför många begäranden): Inte tillämpligt.

16.d. Ange antal personuppgiftsansvariga som inte lämnade några siffror för denna fråga (men som svarade på frågeformuläret och de andra frågorna).
1

17.a. För fråga 1.10 i frågeformuläret för personuppgiftsansvariga, för hur många år bad ni personuppgiftsansvariga att tillhandahålla siffror (välj ett):
☒ 1 år ☐ 3 år ☐ Annat (om så, specificera): Inte tillämpligt.

17.b. Vilken procentandel av de mottagna begärandena om radering var kopplad till samma registrerades utövande av rätten att göra invändningar enligt artikel 21 i dataskyddsförordningen (inklusive invändning mot marknadsföring)? *Ange antalet svarande personuppgiftsansvariga på de relevanta raderna baserat på de siffror som ni har samlat in.* (Fråga 1.10 i i frågeformuläret)

	2024*	**2023**	**2022**
0%	10	Inte tillämpligt.	Inte tillämpligt.
10%	6	Inte tillämpligt.	Inte tillämpligt.
20%	0	Inte tillämpligt.	Inte tillämpligt.
30%	0	Inte tillämpligt.	Inte tillämpligt.
40%	1	Inte tillämpligt.	Inte tillämpligt.
mer än 50 %	2	Inte tillämpligt.	Inte tillämpligt.

17.c. Ange antal personuppgiftsansvariga som inte lämnade några siffror för denna fråga (men som svarade på frågeformuläret och de andra frågorna).
1

18.a. Under den tidsperiod för vilken ni lämnade information i frågorna 15–17 ovan, vilka kategorier av registrerade var de <u>mest aktiva grupperna</u> som lämnade in begäran om radering till svarande personuppgiftsansvariga? (Fråga 1.11 i frågeformuläret)

a. Potentiella kunder	4
b. Kunder	13
c. Uppdragstagare	1
d. Arbetssökande	7
e. Anställda	5
f. Sökande (av allmännyttiga tjänster)	0
g. Medborgare (för den offentliga sektorn)	4

h. Patienter	2
i. Annat	1 Politiker 1 Okänd kategori

18.b. Var följande grupper överrepresenterade i de inkomna begärandena? (Fråga 1.11.1 i frågeformuläret)

a. Föräldrar eller vårdnadshavare för ett eller flera barns räkning:	6
b. Sårbara personer (t.ex. äldre, asylsökande, etniska minoriteter, personer med funktionsnedsättning) eller vårdnadshavare för ett sårbart ämne:	4

18.c. Anser ni att de resultat som ni har fått för denna fråga är konsekventa, med tanke på de svarande personuppgiftsansvarigas sektor och behandlingsverksamhet?
De resultat som vi fått för denna fråga är delvis inkonsekventa med tanke på de svarandes sektorer och behandlingsverksamheter.

En inkonsekvens gäller antalet inkomna begärande generellt, vilket förefaller vara väl lågt, i ljuset av storleken på verksamheterna och antalet registrerade som berörs av deras behandlingar. Detta gäller särskilt de respondenter som är stora företag. En möjlig godtagbar förklaring till det låga antalet begäranden är att flera av respondenterna omfattas av lagstadgade krav på dokumentation, till exempel enligt arkivlagen, patientdatalagen eller apoteksdatalagen. Det är tänkbart att de registrerade är medvetna om dessa krav och därför avstår från att begära radering. En alternativ förklaring är att faktiska begäranden om radering inte hanteras och/eller registreras korrekt. En annan förklaring är att de registrerade inte har fått tillräcklig information om sina rättigheter.

En annan observation som pekar på en inkonsekvens är att ett flertal respondenter uppger att de endast fått in begäranden från kategori av registrerade i form av kunder, patienter och medborgare, men inte anställda eller arbetssökande. Detta trots att de är stora arbetsgivare.

Resultatet visar att det finns variation i hur många begäranden som avslås. Majoriteten av respondenterna inom offentlig sektor uppger att mer än hälften av begärandena avslås, vilket framstår som rimligt eftersom dessa verksamheter omfattas av dokumentationskrav som förhindrar radering. Samtidigt har två hälso- och sjukvårdsverksamheter rapporterat en låg avslagsnivå trots att de omfattas av dokumentationskrav. Detta skapar en inkonsekvens i resultatet sett till de personuppgiftsansvarigas sektor och behandlingsverksamhet. Bland verksamheter som uppgett en låg avslagsnivå återfinns de verksamheter som bedriver kollektivtrafik. För dessa respondenter kan det antas att de stödjer sin personuppgiftbehandling på rättsliga grunder som ger rätt till radering, vilket gör resultatet mer konsekvent i sammanhanget. Två hälso- och sjukvårdsverksamheter har uppgett låg avslagsnivå

trots att de omfattas av dokumentationskrav, dessa resultat framstår som inkonsekventa utifrån de personuppgiftsansvarigas sektor och behandlingsverksamhet.

Flera respondenter uppger att ingen mottagen begäran har gällt rätten till invändning enligt artikel 21. Detta är konsekvent för verksamheter som till största del grundar sin personuppgiftsbehandling på rättslig förpliktelse utifrån lagstadgade dokumentationskrav. I övriga fall kan det däremot tyda på att verksamheten saknar rutiner för att kategorisera begäranden eller att relevant statistik inte finns tillgänglig. En annan förklaring är att de registrerade inte har fått tillräcklig information om sina rättigheter.

Del II – Materiella frågor rörande personuppgiftsansvarigas efterlevnadsnivå

19. Vad är ert allmänna intryck av graden av efterlevnad hos de personuppgiftsansvariga som ni konsulterade när det gäller bestämmelserna i dataskyddsförordningen om rätten till radering?
☐ a. Mycket hög
☐ b. Hög
☐ c. Genomsnitt
☐ d. Låg
☐ e. Mycket låg
☒ f. För olika nivåer för att kvalificera

20. Identifierade ni några betydande skillnader när det gäller olika typer av personuppgiftsansvariga (t.ex. mellan offentlig och privat sektor, storlek osv.), och i så fall vilka?
Nej.

Arbetsflöde för svarande personuppgiftsansvariga

21. Förklara det eller de viktigaste problemen eller utmaningarna (t.ex. ett till tre problem som ni har identifierat (i förekommande fall)) i era utvärderingar/åtgärder med avseende på frågorna 2.1 till 2.9 (rörande interna förfaranden, intern organisation och utbildning, hantering av begäranden osv.) i frågeformuläret för personuppgiftsansvariga. Gör detta på följande vis: a) Namnge det eller de problem som identifierats och beskriv dem kortfattat; b) Vilka bestämmelser i dataskyddsförordningen (eller nationell lagstiftning) berörs av detta? c) Har ni identifierat en möjlig förklaring till varför detta har varit ett problem för vissa eller alla av de svarande personuppgiftsansvariga? d) Vilka skillnader har ni stött på mellan personuppgiftsansvariga i ert land? e) Vilka möjliga lösningar på denna fråga för de svarande personuppgiftsansvariga och/eller de deltagande tillsynsmyndigheterna finns (t.ex. uppföljningsåtgärder)?

Utmaning: Avsaknad av eller otillräckliga interna rutiner och processer
En central utmaning är att många personuppgiftsansvariga förefaller sakna tillräckligt utvecklade och dokumenterade interna rutiner för att hantera en begäran om radering. Många har inte lämnat in någon dokumentation alls, eller endast ett ofullständigt underlag, trots att detta var obligatoriskt om sådana fanns. Ofta hanteras ärenden manuellt och från fall till fall, vilket gör processen personberoende och inkonsekvent. Det finns även oklarheter i ansvarsfördelningen, där till exempel dataskyddsombud

felaktigt tar beslut, vilket strider mot deras oberoende roll. Sammantaget tyder detta på att rutinerna inte är tillräckligt tydliga eller enhetliga för att garantera en korrekt och effektiv hantering.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 e, 5.1 f, 5.2, 12.3, 17 och 24.

En **möjlig förklaring** är en kombination av bristande prioritering och en huvudsakligen manuell hantering. När fasta rutiner och systemstöd saknas blir processen ineffektiv, personberoende och svår att följa upp, särskilt vid en större mängd förfrågningar.

Skillnader som har identifierats är att vissa verksamheter har välfungerande processer där jurister och dataskyddsombud är involverade, medan andra har otydliga rutiner och ansvarsfördelning. Det finns också skillnader i hur man verifierar en persons identitet, där tydliga processer ibland saknas helt.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Sådan vägledning bör praktiskt beskriva hur man kan utforma interna processer, till exempel genom att kartlägga system och dataflöden, förtydliga roller och ansvar, samt vilken dokumentation som behövs för att visa att man följer reglerna.

Utmaning: Svårigheter att identifiera vilka uppgifter som ska raderas
En annan utmaning är att personuppgiftsansvariga verkar ha svårt att tekniskt identifiera och lokalisera alla personuppgifter som omfattas av en begäran om radering. Svaren är ofta vaga och beskriver inte hur man säkerställer att alla relevanta uppgifter hittas i olika system. Vissa hänvisar endast till den information som den enskilde har angett, utan att förklara den egna sökprocessen. Detta tyder på att det ofta saknas tekniska verktyg och systematiska metoder för att kunna genomföra en fullständig radering.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 e, 5.1 f, 12.3, 17 och 32.

En **möjlig förklaring** är att dessa frågor inte prioriteras tillräckligt i verksamheterna. Därmed avsätts inte heller tillräckligt med tid och resurser för att utveckla tekniska lösningar eller ta fram de styrdokument och den utbildning som krävs.

Skillnader som har identifierats är stora, särskilt mellan aktörer som omfattas av lagstadgade krav på att bevara information (som arkivlagen) och de som inte gör det. De förstnämnda har ofta mer komplexa förutsättningar, vilket ställer högre krav på tekniskt stöd och juridisk kompetens.

Möjliga lösningar skulle kunna vara tekniska lösningar som underlättar identifieringen av personuppgifter i olika system. Det behövs även vägledning från IMY eller EDPB, dels om hur nationell lagstiftning om bevarande förhåller sig till rätten till radering, dels om hur tekniska lösningar kan användas för att uppfylla kraven.

22. Finns det någon ledande eller bästa praxis hos de personuppgiftsansvariga som har svarat som ni vill dela med er av?
Trots ett begränsat underlag har följande goda exempel på bästa praxis i hanteringen av begäranden om radering identifierats:

- Skapa tydliga och uppdaterade rutiner, styrdokument och checklistor som specificerar vem som gör vad, hur bedömningen går till och vilka kriterier som gäller för radering enligt både artikel 17.1 och 17.3.
- Se till att all personal får grundläggande och återkommande utbildning i dataskydd efter roll och behov, med start vid anställningens början.
- Säkerställ att medarbetare som hanterar raderingar har tillgång till och vid behov tar stöd från experter, exempelvis dataskyddsombud.
- Använd ett ärendehanteringssystem för att registrera och följa upp alla begäranden, och automatisera processen där det är lämpligt.
- Låt en central funktion samordna hanteringen när ett ärende berör flera avdelningar i organisationen.
- Erbjud flera kanaler för att lämna in en begäran, till exempel e-post, telefon, webbformulär eller fysiska besök.
- Bekräfta alltid mottagandet av en begäran och be om kompletterande information om den är otydlig.
- Kontrollera endast den sökandes identitet vid rimlig osäkerhet. Använd då metoder som är proportionerliga utifrån uppgifternas och situationens beskaffenhet (såsom BankID (inklusive tjänster som kräver sådan inloggning och verifiering), REK-brev, brev till folkbokföringsadressen, , fysisk ID-kontroll på plats eller kontrollfrågor).
- Hantera ärenden i genomsnitt väl inom den yttre tidsfristen om en månad, såsom två veckor, samt informera proaktivt om eventuella förseningar.
- Ge alltid en tydlig motivering med hänvisning till relevanta bestämmelser vid ett avslag på en begäran.
- Informera på eget initiativ andra mottagare av personuppgifterna om att en radering har genomförts.
- Se till att personuppgiftsbiträdesavtal reglerar hur radering ska ske och ge tydliga instruktioner till biträdet när en radering ska utföras.

Villkor för utövandet av rätten till radering och undantag från rätten till radering (fallscenarion)

23. Förklara det eller de viktigaste problemen eller utmaningarna (t.ex. ett till tre problem som ni har identifierat (i förekommande fall)) i era utvärderingar/åtgärder med avseende på frågorna 3.1 till 3.11 i frågeformuläret för personuppgiftsansvariga. Besvara i detta delfrågorna a – e i fråga 21.

Utmaning: Felaktig hantering när en begäran om radering nekas

En utmaning är att flera personuppgiftsansvariga inte vidtar tillräckliga åtgärder när de nekar en begäran om radering. Många uppger att de ofta nekar radering med hänvisning till undantag i dataskyddsförordningen, till exempel för att uppfylla en rättslig förpliktelse eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Trots detta vidtar de sällan några andra skyddsåtgärder, som att begränsa behandlingen av personuppgifterna. Detta tyder på en bristande förståelse för att man på eget initiativ behöver skydda den enskildes rättigheter, även när en begäran om radering inte kan beviljas direkt.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 a, 5.1 e, 5.2, 17.3, 18 och 24.

En **möjlig förklaring** är en bristande förståelse för hur rätten till radering förhåller sig till andra rättigheter, som rätten till begränsning av behandling. Det finns en osäkerhet kring hur man praktiskt kan skydda den registrerades rättigheter när radering inte är ett omedelbart alternativ.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från Europeiska dataskyddsstyrelsen (EDPB). Sådan vägledning bör ur ett praktiskt perspektiv förklara hur rätten till radering samspelar med rätten till begränsning och hur personuppgiftsansvariga kan utforma sina rutiner för att hantera dessa situationer.

Utmaning: Missförstånd kring anmälningsskyldigheten
En annan utmaning är att många personuppgiftsansvariga inte verkar förstå sin skyldighet att underrätta mottagare av personuppgifter om att uppgifter har raderats. Svaren visar på flera missförstånd. Vissa menar att skyldigheten inte varit aktuell, medan andra tror att den endast gäller om den enskilde uttryckligen begär det. Några underrättar endast interna mottagare, och andra endast vissa externa mottagare. Detta indikerar att en majoritet inte förstår att de har en skyldighet att underrätta samtliga mottagare, både interna och externa, utan en specifik begäran från den registrerade.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.2, 17, 19 och 24.

En **möjlig förklaring** är bristande förståelse för anmälningsskyldighetens omfattning och syfte enligt artikel 19. De personuppgiftsansvariga verkar osäkra på hur skyldigheten ska tillämpas i praktiken.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Vägledningen bör klargöra hur personuppgiftsansvariga praktiskt ska utforma sina processer för att uppfylla anmälningsskyldigheten och hur de bör informera den registrerade om detta.

Utmaning: Okunskap om radering vid intresseavvägning
En ytterligare utmaning är att få personuppgiftsansvariga verkar någonsin ha nekat en begäran om radering med hänvisning till att deras berättigade skäl väger tyngre än den enskildes. Detta kan vara en indikation på att den ursprungliga grunden för behandlingen, det vill säga intresseavvägningen, inte har varit tillräckligt stark från början för att utgöra en giltig rättslig grund. Om det sällan finns skäl som väger tyngre än den enskildes intresse av radering, kan det ifrågasättas om det från början fanns ett berättigat intresse som var starkt nog för att motivera behandlingen.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 a, 5.2, 6.1 f, 17.1 c och 24.

En **möjlig förklaring** är bristande förståelse för hur rätten till radering och invändning samspelar med den rättsliga grunden berättigat intresse.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB om rätten till radering och hur den förhåller sig till intresseavvägning enligt artikel 6.1 f.

Utmaning: Upplevd komplexitet och osäkerhet i offentlig sektor
En särskild utmaning för offentlig sektor är att rätten till radering sällan blir aktuell. En stor del av deras personuppgiftsbehandling styrs av annan lagstiftning, såsom

arkivlagar, vilket gör att undantagen i dataskyddsförordningen ofta gäller. Rättsläget upplevs som komplicerat och det finns en osäkerhet kring hur dataskyddsförordningen och nationell lagstiftning förhåller sig till varandra. Eftersom myndigheters beslut kan överklagas ställs höga krav på motiveringar, vilket kräver en trygghet i rättstillämpningen som många verkar sakna.

Bestämmelser som berörs i dataskyddsförordningen och nationell lagstiftning är artiklarna 6.1, 17.3, 19 samt 7 kap. 2 § dataskyddslagen.

En **möjlig förklaring** är att eftersom radering sällan är aktuellt, byggs ingen kunskap eller erfarenhet upp inom verksamheten gällande rätten till radering. Det blir då svårt att motivera att resurser läggs på kompetensutveckling inom området.

Skillnader som har identifierats är att vissa verksamheter har en aktiv involvering av dataskyddsombud och jurister, medan andra ger oklara svar om hur bedömningar görs. Det finns även olika rutiner för att hantera en kombinerad begäran om tillgång och radering.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB som tydliggör hur rätten till radering ska hanteras inom offentlig sektor, med hänsyn till nationell lagstiftning.

24. Finns det någon ledande eller bästa praxis hos de personuppgiftsansvariga som har svarat som ni vill dela med er av?
Trots att få svarande lämnat detaljerade svar har följande goda exempel och rekommendationer för hanteringen av raderingsärenden identifierats:

- Hantera begäranden i rätt ordning. När någon begär både tillgång till och radering av sina uppgifter samtidigt, hantera först begäran om tillgång och därefter begäran om radering.
- Gör alltid en individuell prövning. Bedöm varje begäran om radering för sig, även om verksamheten i huvudsak omfattas av undantag som begränsar rätten till radering.
- Skapa rutiner för att informera mottagare. Se till att på eget initiativ meddela andra mottagare (enligt artikel 19) när personuppgifter har raderats, även om det kan vara tekniskt utmanande.
- Begränsa åtkomsten när radering inte är möjlig. Om personuppgifter inte kan raderas direkt, bör åtkomsten till dem begränsas i väntan på att radering kan ske.
- Dokumentera och ta hjälp vid behov. Dokumentera alla beslut och konsultera dataskyddsombud eller annan expert vid svåra eller komplicerade bedömningar.

Frågor till myndigheter (ingår ej i EDPB:s formulär)

3a. Vilka slutsatser kan dras av svaren på de särskilda frågorna till myndigheter (fråga 3a.1-3a.2.2.1 i frågeformuläret)?
Sverige har infört kompletterande nationell lagstiftning till dataskyddsförordningen som anger att beslut enligt artiklarna 12.5 och 15–21 i EU:s dataskyddsförordning som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till

allmän förvaltningsdomstol.[3] Myndigheter är även skyldiga enligt nationell lagstiftning att motivera sådana beslut.[4]

För att undersöka hur väl dessa regler efterlevs, och hur kraven på motivering och överklagbarhet hanteras, har IMY inom ramen för sin undersökning begärt in information från de verksamheter som omfattas av reglerna.

Respondenterna förefaller ha en hög medvetenhet om sina skyldigheter beträffande rätten till motivering och att överklaga gällande begäranden om radering. Majoriteten har redan identifierat att deras beslut kan överklagas och implementerat konkreta verktyg, såsom beslutsmallar, för att säkerställa att enskilde får både motivering och tydlig information om hur man överklagar.

Samtidigt förefaller det finnas en betydande osäkerhet i verksamheter med mer komplexa organisationsformer. När en verksamhet har inslag av både privat och offentlig styrning (till exempel ett aktiebolag som förvaltas av en offentlig nämnd) blir tillämpningen av kravet på överklagbara beslut oklar.

Resultatet visar att ytterst få avslagsbeslut överklagas, vilket kan tolkas på två sätt. Antingen är de offentliga aktörernas beslut så välmotiverade att den enskilde förstår och accepterar avslaget. Alternativt kan det tyda på att enskilda har låg kännedom om möjligheten att överklaga, och vad det kan leda till.

Kommunikation med registrerade

25. Förklara det eller de viktigaste problemen eller utmaningarna (t.ex. ett till tre problem som ni har identifierat (i förekommande fall)) i era utvärderingar/åtgärder med avseende på frågorna 4.1 till 4.5 i frågeformuläret för personuppgiftsansvariga. Besvara i detta delfrågorna a – e i fråga 21.

Utmaning: Otillräcklig anpassning av svarskanal efter informationens känslighet

En ytterligare utmaning är att personuppgiftsansvariga inte alltid anpassar svarskanalen efter hur känsliga personuppgifterna är. Vissa använder säkrare metoder som rekommenderad post eller säkra digitala vårdtjänster, men detta är inte en självklarhet för alla. Detta tyder på en bristande medvetenhet om informationssäkerhet och att det kan saknas rutiner för riskbedömning.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 f, 12, 17, 24 och 32.

En **möjlig förklaring** är en allmän brist på medvetenhet kring informationssäkerhet. Det kan också bero på att det saknas tydliga interna rutiner för hur man ska bedöma risker och välja en lämplig och säker kommunikationskanal i varje enskilt fall.

Skillnader som har identifierats är att rutinerna varierar stort. Vissa verksamheter anpassar svarskanalen efter informationens känslighet, medan andra inte verkar göra denna bedömning.

[3] 7 kap. 2 § Lagen om kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218)
[4] 32 § Förvaltningslagen (2017:900)

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Vägledningen bör klargöra vikten av att göra en riskbedömning och välja en svarskanal som skyddar den enskildes personuppgifter på ett lämpligt sätt.

Utmaning: Bristfällig information om handläggningstid
En annan utmaning är att de flesta personuppgiftsansvariga inte informerar om den förväntade handläggningstiden när de tar emot en begäran om radering. Även om många skickar en mottagningsbekräftelse, är det få som anger hur lång tid hanteringen kan ta. Detta kan påverka öppenheten och den enskildes förväntningar negativt.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 a, 12, 17 och 24.

En **möjlig förklaring** är att det inte finns något uttryckligt lagkrav på att informera om handläggningstid. Därför blir detta inte en prioriterad åtgärd i verksamheterna.

Skillnader som har identifierats är små, då nästan ingen av de svarande uppger att de regelbundet informerar om handläggningstiden.

Möjliga lösningar skulle kunna vara vägledning från EDPB. Vägledningen skulle kunna betona vikten av att informera om handläggningstider som en del av god praxis för att upprätthålla transparens gentemot den registrerade.

Utmaning: Bristande flexibilitet i kommunikationskanaler
En utmaning förefaller vara att även om en begäran om radering ofta tas emot via flera olika kanaler, besvaras de bara genom en eller ett fåtal av dessa. Detta kan tyda på att hänsyn inte alltid tas till den registrerades önskemål om kommunikationskanal. Det finns en risk att kommunikationen inte är tillräckligt tydlig och lättillgänglig, och att man inte gör det tillräckligt enkelt för enskilda att utöva sina rättigheter.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 12, 17 och 24.

En **möjlig förklaring** är att det saknas resurser och prioriteringar för att samordna kommunikationskanalerna. Det kan också bero på en avsaknad av tekniska system, som en integritetsportal, som kan hantera både mottagande och besvarande av en begäran på ett flexibelt sätt som passar den enskildes behov och samtidigt säkerställer en lämplig säkerhetsnivå.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Sådan vägledning bör ur ett praktiskt perspektiv förklara hur personuppgiftsansvariga kan skapa effektiva och flexibla kanaler för att ta emot och besvara en begäran om radering som dels kan ta hänsyn till den enskildes behov, dels kan säkerställa en lämplig säkerhetsnivå och hur en sådan bedömning kan göras.

26. Finns det någon ledande eller bästa praxis hos de personuppgiftsansvariga som har svarat som ni vill dela med er av?
Baserat på de svar som inkommit har följande goda exempel och rekommendationer för information och kommunikation kring radering identifierats:

- Var tydlig i integritetspolicyn. Ange både de kriterier som bestämmer hur länge personuppgifter sparas och, om möjligt, den exakta lagringstiden.
- Erbjud tydlig information och flera kontaktvägar. Informera lättillgängligt, till exempel på webbplatsen, om hur man begär radering. Gör det möjligt att skicka in en begäran via flera kanaler, såsom e-post, telefon, webbformulär eller fysiskt besök.
- Var flexibel och proportionerlig med identitetskontroll. Använd metoder för att säkerställa en persons identitet som är proportionerliga med hänsyn till uppgifternas och situationens beskaffenhet (till exempel BankID, ID-kontroll på plats eller ett brev som skickas till folkbokföringsadressen).
- Bekräfta alltid att begäran tagits emot. Skicka en mottagningsbekräftelse och informera gärna samtidigt om den förväntade handläggningstiden.
- Välj en säker svarskanal. Anpassa kanalen för svar utifrån hur begäran kom in och vilken information som svaret innehåller, med hänsyn till informationssäkerheten.

Tekniska aspekter

27. Förklara det eller de viktigaste problemen eller utmaningarna (t.ex. ett till tre problem som ni har identifierat (i förekommande fall)) i era utvärderingar/åtgärder med avseende på frågorna 5.1 till 5.6 i frågeformuläret för personuppgiftsansvariga. Besvara i detta delfrågorna a – e i fråga 21.

Utmaning: Osäkerhet kring radering i säkerhetskopior

Radering av personuppgifter i säkerhetskopior görs enligt många personuppgiftsansvariga enligt separata rutiner där radering sker, men över en längre tidsperiod. Detta skapar en utmaning i form av en osäkerhet om raderingen i enlighet med sådana separata rutiner vid en enskild begäran verkligen sker fullständigt omedelbart och ”utan onödigt dröjsmål” som dataskyddsförordningen kräver.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.1 f, 17 och 24 samt 32.1 c och 32.2.

En **möjlig förklaring** är att samtidigt som personuppgiftsansvariga ska uppfylla kraven i artikel 17 om radering, ska de också ta hänsyn till säkerheten i samband med behandlingen av personuppgifter i artikel 32. Detta så att uppgifterna är skyddade från förstöring, förlust eller ändring under tiden som de behandlas, samt att tillgänglighet och tillgång kan återställas i rimlig tid efter en fysisk eller teknisk incident.

En generell utmaning för personuppgiftsansvariga och personuppgiftsbiträden när det gäller säkerhetskopior är att tekniskt inte kunna återläsa dessa vid behov efter en fysisk eller teknisk incident.

För att i nästa steg samtidigt säkerställa att raderingen kvarstår efter en återläsning, är det viktigt med interna rutiner för att i säkerhetskopiorna flagga att poster med personuppgifter som raderats i de operativa informationssystemen inte ska läsas tillbaka.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Vägledningen bör förklara hur personuppgiftsansvariga praktiskt ska hantera radering i säkerhetskopior och vad som menas med "utan onödigt dröjsmål" i detta sammanhang.

Utmaning: Användning av anonymisering istället för radering
En annan utmaning är att flera personuppgiftsansvariga uppfyller en begäran om radering genom att istället anonymisera uppgifterna, till exempel för att fortsatt kunna använda dem för analyser. Detta skapar en risk att en faktisk radering av personuppgifterna inte utförs fullt ut enligt lagens krav.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 6, 7 och 17.

En **möjlig förklaring** är en önskan att behålla data för andra ändamål, såsom statistik eller analys, i kombination med en osäkerhet kring vad som juridiskt och tekniskt utgör en fullständig radering jämfört med en effektiv anonymisering.

För anonymisering följer ytterligare en utmaning i hanteringen av risken med personuppgiftsbehandlingen om denna inte genomförts på ett sådant sätt att den registrerade inte längre är identifierbar.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning och rekommendationer från EDPB. Vägledningen bör klargöra skillnaden mellan radering och anonymisering och under vilka förutsättningar anonymisering kan anses uppfylla raderingskravet. Detta kan t.ex. ske i de planerade kommande riktlinjerna om anonymisering från EDPB.

Utmaning: Avsaknad av interna processer och riktlinjer
En ytterligare utmaning är att många organisationer saknar tydliga interna instruktioner och fastställda processer för att hantera en begäran om radering. Detta leder till att arbetet blir ineffektivt och att hanteringen kan skilja sig åt inom samma organisation. Utan systematik är det svårt att säkerställa att alla uppgifter som ska raderas verkligen hittas och tas bort. Respondenter hänvisar dock till internationella standarder i sina svar, som exempelvis dem inom ISO/IEC 27000-serien.

Bestämmelser som berörs i dataskyddsförordningen är artiklarna 5.2, 17, 24 och 32.

En **möjlig förklaring** är att frågan inte har prioriterats tillräckligt för att man ska ha avsatt resurser för att skapa tydliga policyer, rutiner och utbildningsinsatser.

Skillnader som har identifierats är att organisationer som hanterar många begäranden om radering oftare har utvecklat en automatiserad och enhetlig process. Det framkommer också att ansvaret för att hantera förfrågningar kan ligga på olika avdelningar, vilket bidrar till oenhetlig praxis.

Möjliga lösningar skulle kunna vara att tillsynsmyndigheter erbjuder stöd och råd, till exempel genom att hänvisa till internationella standarder för informationssäkerhet (som ISO/IEC)[5]. Till detta kan även tilläggas hänvisning till praktiska nationella ramverk, så som MSB:s metodstöd för informations- och cybersäkerhet. Detta för att ge vägledning till stöd för ett riskbaserad och systematiskt informationssäkerhetsarbete vilket stödjer all informationshantering, likväl som radering.

[5] ISO/IEC 27000-serien utgör en samling av standarder för ledningssystem inom informationssäkerhet, cybersäkerhet och integritetsskydd. Samlingen består av två typer av standarder – ett för ledningssystem i syfte att stödja ett systematiskt arbetssätt och ett för vägledning med fokus på säkerhetsåtgärder i syfta att skydda informationen. Serien inkluderar bland annat även standarder för vägledning om riskhantering inom informationssäkerhet samt säkerhetstekniker för hantering av personuppgifter.

Utmaning: Svårigheter att verifiera den registrerades identitet
En specifik utmaning som framförs är svårigheten att säkert identifiera att personen som begär radering verkligen är den registrerade, och inte en obehörig som utger sig för att vara denne. Detta skapar en säkerhetsrisk och en svår avvägning för den personuppgiftsansvarige.

Bestämmelser som berörs i dataskyddsförordningen är artikel 12.

En **möjlig förklaring** är den inneboende konflikten mellan att göra det enkelt för enskilda att utöva sina rättigheter och behovet av att skydda personuppgifter från obehörig åtkomst, förlust, förstöring eller ändring.

Inga tydliga **skillnader** har kunnat identifieras mellan de personuppgiftsansvariga.

Möjliga lösningar skulle kunna vara vägledning från EDPB om praktiska och proportionerliga metoder för att verifiera en persons identitet. Vägledningen bör hjälpa personuppgiftsansvariga att hitta en balans som är säker men inte orimligt betungande för den enskilde.

28. Finns det någon ledande eller bästa praxis hos de personuppgiftsansvariga som har svarat som ni vill dela med er av?
Även om underlaget om de tekniska aspekterna är begränsat, har följande goda exempel och rekommendationer för att genomföra radering identifierats:

- Skapa tydliga interna styrdokument. Dokumentera processen för radering och vilka rättsliga grunder som styr bevarandet av olika uppgifter. Tydliga, interna regler och processer skapar en mer enhetlig hantering.
- Automatisera där det är möjligt. Använd centraliserade system och tekniska verktyg för att automatisera både hanteringen av en begäran och själva raderingen. Det minskar risken för manuella fel och gör processen effektivare.
- Erbjud en digital portal för ärendehantering. En portal, "mina sidor" eller liknande ökar säkerheten vid identifiering och ger enskilda möjlighet att följa statusen på sina ärenden.
- Verifiera att raderingen genomförts. Inför rutiner och tekniska kontroller för att testa och verifiera att de uppgifter som skulle raderas faktiskt är permanent borta.
- Överväg anonymisering som metod. Genom att ta bort alla identifierare kan data användas för statistik och analys utan att längre klassas som personuppgifter. Detta kan vara ett effektivt sätt att uppfylla en begäran och samtidigt behålla värdefull information som inte är personuppgifter.
- Följ etablerade standarder. Använd ramverk som ISO 27000-serien som vägledning för hur information ska identifieras, raderas och förstöras på ett säkert och strukturerat sätt.

Del III – De deltagande tillsynsmyndigheternas åtgärder

29. Har ni redan offentliggjort vägledning (t.ex. faktablad, riktlinjer, frågor och svar, utbildning) om genomförandet av rätten till radering? Ange eventuella allmänna eller riktade riktlinjer som ni har antagit (t.ex. barns rätt till radering, rätt till radering i specifika sammanhang, t.ex. online eller för kreditbedömning), även *innan* CEF inleddes? Om ja, ange namn, datum, länk till vägledningen och en kort beskrivning av vägledningen.
Vi har allmän information på vår webbplats om vad rätten till radering innebär: Rätt till radering av dina personuppgifter | IMY:
https://www.imy.se/privatperson/dataskydd/dina-rattigheter/radering/

30. Har ni vidtagit några åtgärder (dvs. faktainsamlingar, informella kontakter, föregående samråd, utredningar *på eget initiativ eller* klagomålsbaserade utredningar och verkställighetsåtgärder, t.ex. fall där er tillsynsmyndighet utfärdade ett föreläggande om att radera personuppgifter eller begränsa behandlingen och anmäla åtgärder till mottagare (artikel 58.2 g i dataskyddsförordningen)) gentemot personuppgiftsansvariga om rätten till radering *innan CEF 2025 inleddes?* Ge en kort översikt över de åtgärder ni har vidtagit och resultatet av dessa åtgärder.
Efter att ha utövat tillsyn mot Google utfärdade IMY år 2020 en sanktionsavgift på 75 miljoner kronor för att Google bristfälligt hade hanterat registrerades rätt att få sökresultat borttagna: https://www.imy.se/tillsyner/google/. Kammarrätten sänkte sanktionsavgiften till 50 miljoner kronor.

31. Kan ni ge information om de klagomål som ni har mottagit angående rätten till radering sedan dataskyddsförordningen trädde i kraft? (t.ex. antal klagomål gällande artikel 17 i dataskyddsförordningen, antal klagomål i denna fråga i jämförelse med övriga klagomål, växande antal klagomål, hantering av dessa klagomål etc.)?
Vi för ingen exakt statistik över vilka artiklar som klagomål gäller. Däremot bedöms en stor del klagomål ha gällt artikel 17, särskilt beträffande så kallade söktjänster.

32. Vilka eventuella åtgärder överväger ni att vidta på grundval av resultaten av denna CEF gentemot de personuppgiftsansvariga som kontaktats? (t.ex. skrivelse, rekommendationer till den personuppgiftsansvarige, ytterligare vägledning, korrigerande åtgärder såsom förelägganden, förelägganden med eller utan en inkrementell sanktion, administrativa sanktionsavgifter). Ange om möjligt tidsplanen för dessa åtgärder (även om formella utredningar fortfarande pågår).
Inga särskilda åtgärder mot de som kontaktats övervägs i nuläget.

33. Mot bakgrund av era resultat i denna CEF, överväger ni att, *på er tillsynsmyndighets nivå*, vidta åtgärder för att kommunicera och öka medvetenheten om rätten till radering?
☒ Ja ☐ Nej

33.a. Om ja på föregående fråga, ange vilka av följande åtgärder som ni anser vara att föredra?
☒ a. Mer vägledning på nätet
☐ b. Utbildningstillfällen online eller på distans
☐ c. Anordnade konferenser

☒ d. Övrigt (om så, specificera): IMY kommer att i ljuset av de slutsatser som EDPB kommer fram till i sin rapport, överväga att ta fram vägledning och rekommendationer anpassade efter nationella förhållanden.

34. Bör fler åtgärder vidtas på EDPB-nivå när det gäller rätten till radering, och om ja, vilka åtgärder skulle vara att föredra? Om det behövs, vänligen specificera de aspekter av rätten till radering som skulle kunna utvecklas.
☐ Nej ☒ Ja (om så, specificera):

Vägledning och rekommendationer. Särskilt från ett mer proaktivt och praktiskt perspektiv. Följande bör beröras:

- Hur personuppgiftsansvariga kan kartlägga sina system och dataflöden vilket kan underlätta hanteringen av begäranden om radering.
- Vilket systemstöd, verktyg och övrig automatisering samt intern rollfördelning som kan underlätta vid hanteringen av begäranden om radering.
- Hur rätten till radering förhåller sig till exempelvis på förhand bestämda lagringsperioder.
- Vilken dokumentation och information som bör lämnas till registrerade, särskilt vid mer automatiserade processer.
- Mer information om hur rätten till radering ska förstås och implementeras, särskilt avseende hur begränsningarna och undantagen bör tolkas.
- Hur rätten till radering förhåller sig till de andra rättigheterna i artiklarna 18–19, särskilt från ett mer praktiskt perspektiv med rekommendationer om hur personuppgiftsansvariga bör utforma sina rutiner/processer, system och information till den registrerade.
- Hur personuppgiftsansvariga förväntas utforma sina raderingsprocesser, särskilt avseende säkerhetskopior.
- Hur anonymisering skulle kunna anses uppfylla kravet på radering.
- Hur radering ”utan onödigt dröjsmål” i artikel 17 ska tolkas.

35. Finns det några andra observationer som ni vill dela med er av?
IMY vill lyfta fram de erfarenheter som om utmaningar och önskemål om vägledning som respondenterna själva har lyft fram (se nedan, svaret på fråga 36 och 37).

Utöver detta vill IMY lyfta att vi inom ramen för undersökningen även har ställt frågor till respondenter som berörs av viss nationell lagstiftning som kompletterar bestämmelserna om rätten till radering i dataskyddsförordningen. Sverige har infört kompletterande nationell lagstiftning till dataskyddsförordningen som anger att beslut enligt artiklarna 12.5 och 15–21 i EU:s dataskyddsförordning som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.[6] Myndigheter är även skyldiga enligt nationell lagstiftning att motivera sådana beslut.[7]

Inom ramen för denna undersökning har IMY begärt in information för att bedöma hur väl dessa regler efterlevs, särskilt vad gäller rätten till motivering och möjligheten att överklaga. Resultatet visar att de flesta av de berörda verksamheterna har god medvetenhet om sina skyldigheter. Många har också tagit fram konkreta verktyg, som beslutsmallar, för att säkerställa att den enskilde får tydlig motivering och information om hur ett avslag kan överklagas. Samtidigt förefaller det finnas en betydande osäkerhet i verksamheter med mer komplexa organisationsformer. När en verksamhet

[6] 7 kap. 2 § Lagen om kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218)
[7] 32 § Förvaltningslagen (2017:900)

har inslag av både privat och offentlig styrning (till exempel ett aktiebolag som förvaltas av en offentlig nämnd) är det oklart hur kravet på överklagbara beslut ska tillämpas. Resultatet visar att ytterst få avslagsbeslut överklagas till förvaltningsdomstol, vilket kan tolkas på två sätt. Antingen är de offentliga aktörernas beslut så välmotiverade att den enskilde förstår och accepterar avslaget. Alternativt kan det tyda på att enskilda har låg kännedom om möjligheten att överklaga, och vad det kan leda till.

Sammantaget visar resultaten att det finns en god medvetenhet bland de berörda respondenterna om deras skyldigheter enligt den nationella lagstiftningen. Samtidigt kvarstår vissa utmaningar och IMY ser ett fortsatt behov av vägledning riktad särskilt till myndigheter.

Del IV – Respondenternas erfarenheter (ingår ej i EDPB:s formulär)

36. Vilka juridiska, tekniska och/eller organisatoriska utmaningar har respondenterna i huvudsak angett att de ställs inför vid genomförandet av rätten till radering enligt artikel 17 i dataskyddsförordningen?
Respondenterna i undersökningen har i identifierat flera juridiska, tekniska och organisatoriska utmaningar med att uppfylla rätten till radering.

När det gäller **juridiska och kommunikativa utmaningar** är särskilt följande framträdande:

- Att balansera rätten till radering mot andra lagar, som bokföringslagen, som kräver att uppgifter sparas.
- Att avgöra den exakta tidpunkten när personuppgifter får raderas, till exempel efter att en rättsprocess har avslutats.
- Att på ett enkelt sätt förklara för enskilda varför rätten till radering inte är absolut och varför en begäran kan avslås.
- Att hantera den begreppsförvirring som uppstår när rätten till radering blandas ihop med andra rättigheter, som tillgång till allmänna handlingar.

När det gäller **tekniska utmaningar** är särskilt följande framträdande:

- Att lokalisera en persons alla uppgifter när de är spridda över många olika IT-system som saknar centrala sökfunktioner.
- Att det är komplicerat och dyrt att utveckla och underhålla automatiska processer för radering, särskilt om antalet ärenden är få.

När det gäller **organisatoriska utmaningar** är särskilt följande framträdande:

- Att processen för radering ofta kräver mycket tid och manuellt arbete, från att identifiera en person till att kontrollera att allt är borta.
- Att samordna raderingen i stora organisationer med flera olika ansvariga, för att säkerställa att alla uppgifter hittas och tas bort.
- Att säkerställa att även externa leverantörer raderar de uppgifter de hanterar, vilket kräver tydliga avtal och uppföljning.

37. Vad har respondenterna i huvudsak angett skulle kunna hjälpa dem vid hanteringen av begäranden om radering (exempel, verktyg, något annat)?
För att underlätta hanteringen av raderingsärenden efterfrågar respondenterna tydligare vägledning och praktiskt stöd, bättre tekniska verktyg samt ökade möjligheter till utbildning och erfarenhetsutbyte.

När det gäller **vägledning och praktiskt stöd** bör detta finnas lättillgängligt och innehålla konkreta exempel på hur rätten till radering ska hanteras i praktiken. Särskilt vore följande önskvärt:

- Tydligare information om vilka personuppgifter som är undantagna från rätten till radering, exempelvis när annan lagstiftning kräver att uppgifter sparas.
- Rekommendationer för hur länge olika typer av vanligt förekommande personuppgifter bör sparas.
- Konkreta råd om hur anonymisering kan användas för att uppfylla kravet på radering.
- Standardiserade mallar för beslut och checklistor som kan användas vid handläggning av ärenden.
- Vägledning som är anpassad för både privat och offentlig sektor, samt för specifika branscher.

När det gäller **tekniska verktyg** vore särskilt följande önskvärt:

- Verktyg som kan automatisera fler delar av processen, vilket minskar behovet av manuellt arbete och förbättrar spårbarheten. AI skulle kunna användas för att effektivisera, säkra och dokumentera processen.
- Bättre verktyg för att kunna söka efter och identifiera en persons uppgifter i alla de olika system där de kan finnas lagrade.
- Tydligare krav på att externa tjänsteleverantörer måste erbjuda system och verktyg med inbyggd funktionalitet som gör det enkelt att tillgodose de registrerades rättigheter.

När det gäller **utbildning och erfarenhetsutbyte** vore särskilt följande önskvärt:

- Fler utbildningsinsatser, särskilt sådana som riktar sig till medarbetare som inte är jurister.
- Skapa forum för erfarenhetsutbyte mellan olika organisationer och branscher, för att kunna lära av varandra och utveckla gemensamma lösningar.