Europeiska unionens
officiella tidning

SV
L-serien

2024/2639

10.10.2024

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/2639

av den 9 oktober 2024

om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2023/988 vad gäller roller och uppgifter för de gemensamma nationella kontaktpunkterna för systemet för snabb varning Safety Gate

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG ([1]), särskilt artikel 25.2 andra stycket, och

av följande skäl:

(1) Förordning (EU) 2023/988 föreskriver att systemet för snabb varning Safety Gate (*Safety Gate-systemet*) är systemet för snabb varning för utbyte av information om korrigerande åtgärder avseende farliga produkter. För att säkerställa ett effektivt informationsflöde och att Safety Gate-systemet fungerar väl, ska enligt artikel 25.2 första stycket i förordning (EU) 2023/988 varje medlemsstat utse en gemensam nationell kontaktpunkt för Safety Gate-systemet (*Safety Gate-kontaktpunkt*). Enligt artikel 25.2 första stycket i förordning (EU) 2023/988 ska Safety Gate-kontaktpunkten åtminstone ansvara för att kontrollera att de anmälningar som inges till kommissionen för validering är fullständiga och för kommunikation med kommissionen om de uppgifter som föreskrivs i artikel 26.1–26.6 i den förordningen. Utseendet av den nationella Safety Gate-kontaktpunkten bör inte påverka medlemsstaternas behörighet att organisera sina marknadskontrollsystem.

(2) Kommissionens genomförandebeslut (EU) 2019/417 ([2]) fastställde riktlinjer för förvaltningen av Europeiska unionens system för snabbt informationsutbyte (Rapex) upprättade enligt det upphävda Europaparlamentets och rådets direktiv 2001/95/EG ([3]). Det genomförandebeslutet fastställer de nationella Rapexkontaktpunkternas uppgifter, inbegripet att organisera och leda de berörda nationella myndigheternas arbete, se till att alla uppgifter utförs korrekt och, i synnerhet, att all information som krävs utan dröjsmål lämnas till kommissionen och att samordna alla nationella verksamheter och initiativ som utförs i samband med systemet. Med hänsyn till de goda erfarenheterna av de nationella Rapexkontaktpunkternas funktion bör Safety Gate-kontaktpunkternas roller och uppgifter i lämpligaste mån innefatta de roller och uppgifter som fastställs i genomförandebeslut (EU) 2019/417.

(3) För att säkerställa ett effektivt informationsflöde mellan Safety Gate-kontaktpunkten och de olika myndigheter som deltar i Safety Gate-systemet i en viss medlemsstat bör Safety Gate-kontaktpunkten organisera och leda arbetet i sitt nätverk av nationella myndigheter som arbetar med Safety Gate-systemet (*nationella Safety Gate-nätverk*).

(4) I linje med sina befintliga uppgifter enligt genomförandebeslut (EU) 2019/417 och för en effektiv användning av Safety Gate-systemet och samstämmighet i den information som lämnas bör Safety Gate-kontaktpunkterna utbilda och bistå de nationella myndigheterna vid användning av systemet.

([1]) EUT L 135, 23.5.2023, s. 1, ELI: http://data.europa.eu/eli/reg/2023/988/oj.

([2]) Kommissionens genomförandebeslut (EU) 2019/417 av den 8 november 2018 om fastställande av riktlinjer för förvaltningen av Europeiska unionens system för snabbt informationsutbyte (Rapex) upprättade enligt artikel 12 i direktiv 2001/95/EG om allmän produktsäkerhet och dess underrättelsesystem (EUT L 73, 15.3.2019, s. 121, ELI: http://data.europa.eu/eli/dec/2019/417/oj).

([3]) Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet (EGT L 11, 15.1.2002, s. 4, ELI: http://data.europa.eu/eli/dir/2001/95/oj).

(5) För att undvika dubblering av anmälningar i Safety Gate-systemet bör Safety Gate-kontaktpunkterna innan de lämnar in en anmälan kontrollera, i tillämpliga fall med hjälp av de nationella myndigheterna, om en åtgärd avseende produkten redan har anmälts i Safety Gate-systemet.

(6) Spindeln för produktsäkerhet eSurveillance är en it-applikation som utvecklats och förvaltas av kommissionen och syftar till att upptäcka produkter som har anmälts i Safety Gate-systemet och som fortfarande säljs eller dyker upp på nytt i nätbutiker och på onlinemarknadsplatser. För att göra marknadskontrollen online effektivare bör användningen av den främjas på bred front, i tillämpliga fall tillsammans med andra liknande verktyg som används av myndigheterna.

(7) Kommissionen och de nationella myndigheterna fungerar som gemensamt personuppgiftsansvariga för behandling av uppgifter i Safety Gate-systemet i enlighet med artikel 26 i Europaparlamentets och rådets förordning (EU) 2016/679 ([4]) och artikel 28 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([5]). Det är därför lämpligt att specificera rollerna och ansvarsområdena för varje gemensamt personuppgiftsansvarig.

(8) Denna förordning bör tillämpas från och med den dag då förordning (EU) 2023/988 börjar tillämpas.

(9) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från kommittén för förordningen om allmän produktsäkerhet, som inrättades i enlighet med artikel 46.1 i förordning (EU) 2023/988.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

De gemensamma nationella kontaktpunkterna som avses i artikel 25.2 i förordning (EU) 2023/988 (*Safety Gate-kontaktpunkter*) ska ha följande roller och uppgifter:

a) Kontroll och validering av att anmälningar från andra nationella myndigheter i deras medlemsstat är fullständiga innan anmälningarna i enlighet med artikel 25.2 första stycket i förordning (EU) 2023/988 översänds till kommissionen genom Safety Gate-systemet.

b) Kontroll innan anmälningar lämnas in genom Safety Gate-systemet av huruvida den produkt som anmälan gäller redan har anmälts i det systemet och om så är fallet, och när så är lämpligt i samarbete med den berörda nationella myndigheten, i stället lämna in en uppföljningsanmälan i enlighet med artikel 26.7 i förordning (EU) 2023/988.

c) Säkerställande av att anmälningar från andra medlemsstater som validerats av kommissionen i Safety Gate-systemet når de berörda nationella myndigheterna i deras medlemsstat, inbegripet de myndigheter som ansvarar för kontroller vid de yttre gränserna, för lämplig uppföljning på nationell nivå.

d) Främjande av användningen av spindeln för produktsäkerhet eSurveillance i deras medlemsstat, och andra liknande verktyg när så är relevant, och särskilt de nationella myndigheternas uppföljning av relevanta resultat.

e) Utbildning av och bistånd till alla nationella myndigheter vid användning av Safety Gate-systemet.

([4]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) Underlättande av att de arbetsuppgifter i samband med Safety Gate-systemet som härrör från förordning (EU) 2023/988 och kommissionens delegerade förordning av den 27 augusti 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2023/988 vad gäller regler om tillgång till och drift av Safety Gate-systemet för snabb varning, vilken information som ska föras in i det systemet, vilka krav anmälningar ska uppfylla och kriterier för bedömning av risknivån ([6]) utförs i deras medlemsstat och i synnerhet att all den information som krävs lämnas till kommissionen i enlighet med förordning (EU) 2023/988.

g) Samarbete och utbyte av information som är relevant för produktsäkerhet med andra Safety Gate-kontaktpunkter och deltagande i diskussioner mellan Safety Gate-kontaktpunkterna under samordning av kommissionen.

h) Utbyte av information som är relevant för produktsäkerhet på nationell nivå med den myndighet som är medlem i det nätverk för konsumentsäkerhet som avses i artikel 30 i förordning (EU) 2023/988, om den är en annan myndighet än Safety Gate-kontaktpunkten.

i) Utbyte av information som är relevant för produktsäkerhet på nationell nivå med det centrala samordningskontor som utsetts i enlighet med artikel 10 i Europaparlamentets och rådets förordning (EU) 2019/1020 ([7]) och artikel 23.1 i förordning (EU) 2023/988, om det är en annan myndighet än Safety Gate-kontaktpunkten.

j) Upplysning utan dröjsmål till kommissionen om eventuella tekniska problem med Safety Gate-systemets funktion.

k) Hantering av begäranden om åtkomst till applikationer kopplade till Safety Gate-systemet från användare i deras nationella Safety Gate-nätverk, med upplysning till kommissionen om alla personalförändringar som påverkar åtkomsträttigheterna.

l) Svar på begäranden som rör driften av Safety Gate-systemet i deras medlemsstat från berörda parter, inbegripet ekonomiska aktörer och leverantörer av onlinemarknadsplatser.

m) Kontakt med den myndighet i deras medlemsstat som lämnat in den berörda anmälan i Safety Gate-systemet, när så är lämpligt, om eventuell kompletterande information som man skulle kunna överväga att lägga till i anmälan, på begäran av ekonomiska aktörer eller leverantörer av onlinemarknadsplatser, i synnerhet när dessa kan påverkas negativt av en ofullständig anmälan i Safety Gate-systemet.

Artikel 2

När kommissionen och de nationella myndigheterna fungerar som gemensamt personuppgiftsansvariga för behandling av uppgifter i Safety Gate-systemet i enlighet med artikel 26 i förordning (EU) 2016/679 och artikel 28 i förordning (EU) 2018/1725 ska de ha de roller och ansvarsområden som fastställs i bilagan till denna förordning.

([6]) Ännu inte offentliggjord i EUT.

([7]) Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj).

Artikel 3

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 13 december 2024.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 9 oktober 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

GEMENSAMT PERSONUPPGIFTSANSVAR FÖR SYSTEMET FÖR SNABB VARNING SAFETY GATE

1. INNEHÅLL OCH BESKRIVNING AV BEHANDLINGEN

Systemet för snabb varning Safety Gate (*Safety Gate-systemet*) är ett underrättelsesystem som drivs av kommissionen och är avsett för snabbt informationsutbyte mellan nationella myndigheter i medlemsstaterna, de tre staterna i Europeiska ekonomiska samarbetsområdet/Europeiska frihandelssammanslutningen (EES/Efta) (dvs. Island, Liechtenstein och Norge) och kommissionen om åtgärder som vidtagits mot farliga produkter som påträffas på unionsmarknaden och/eller EES/Efta-marknaden.

Syftet med Safety Gate-systemet är att göra det möjligt att snabbt utbyta information om korrigerande åtgärder som vidtagits i hela unionen för produkter som utgör en risk.

Informationsutbytet avser korrigerande åtgärder som vidtagits med avseende på sådana farliga konsumentprodukter och produkter för yrkesmässigt bruk som omfattas av förordningarna (EU) 2023/988 eller (EU) 2019/1020.

Safety Gate-systemet omfattar både åtgärder som åläggs av nationella myndigheter och åtgärder som vidtas frivilligt av ekonomiska aktörer.

2. DET GEMENSAMMA PERSONUPPGIFTSANSVARETS OMFATTNING

Kommissionen och de nationella myndigheterna ska fungera som gemensamt personuppgiftsansvariga för behandlingen av uppgifter i Safety Gate-systemet. Med *nationella myndigheter* avses alla myndigheter som arbetar med produktsäkerhet i medlemsstaterna och/eller Efta/EES-länderna och som deltar i EU:s nätverk av Safety Gate-kontaktpunkter, inbegripet marknadskontrollmyndigheter med ansvar för att övervaka produkters överensstämmelse med säkerhetskraven och myndigheter med ansvar för kontroller vid de yttre gränserna.

För tillämpningen av artikel 26 i förordning (EU) 2016/679 och artikel 28 i förordning (EU) 2018/1725 faller följande behandling under kommissionens ansvar i egenskap av gemensam personuppgiftsansvarig för personuppgifter:

1) Kommissionens behandling av information om åtgärder som vidtagits mot produkter som utgör allvarliga risker och som importeras till eller exporteras från unionen och Europeiska ekonomiska samarbetsområdet, i syfte att vidarebefordra informationen till de gemensamma nationella kontaktpunkterna för Safety Gate-systemet (*Safety Gate-kontaktpunkter*).

2) Kommissionens behandling av information från tredjeländer, internationella organisationer, företag eller andra system för snabb varning om produkter med ursprung i eller utanför EU som utgör en risk för konsumenters hälsa och säkerhet, i syfte att vidarebefordra informationen till de nationella myndigheterna.

När kommissionen utför denna verksamhet ska den se till att de tillämpliga skyldigheterna och villkoren i förordning (EU) 2018/1725 efterlevs.

De nationella myndigheterna ska i egenskap av gemensamt personuppgiftsansvariga ansvara för följande behandling:

1) Nationella myndigheters behandling av information i enlighet med artikel 26 i förordning (EU) 2023/988 om allmän produktsäkerhet och artikel 20 i förordning (EU) 2019/1020 i syfte att anmäla sådan information till kommissionen och andra medlemsstater samt Efta-/EES-länder.

2) Nationella myndigheters behandling av information efter deras uppföljning av anmälningar i Safety Gate-systemet i syfte att anmäla sådan information till kommissionen och andra medlemsstater samt Efta-/EES-länder.

När de nationella myndigheterna utför denna verksamhet ska de se till att de tillämpliga skyldigheterna och villkoren i förordning (EU) 2016/679 efterlevs.

3. DE GEMENSAMT PERSONUPPGIFTSANSVARIGAS ANSVAR, ROLLER OCH FÖRHÅLLANDE GENTEMOT DE REGISTRERADE

3.1 **Kategorier av registrerade och personuppgifter**

De gemensamt personuppgiftsansvariga ska gemensamt behandla följande kategorier av personuppgifter:

a) Kontaktuppgifter för användare av Safety Gate-systemet.

Följande uppgifter får behandlas:

— Förnamn på användare av Safety Gate-systemet.

— Efternamn på användare av Safety Gate-systemet.

— E-postadress till användare av Safety Gate-systemet.

— Land för användare av Safety Gate-systemet.

— Språkpreferens hos användare av Safety Gate-systemet.

b) Kontaktuppgifter till dem som har skrivit och validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

Det kan röra sig om

— Safety Gate-kontaktpunkter och inspektörer från marknadskontrollmyndigheter i medlemsstaterna och Efta-/EES-länderna eller från de nationella myndigheter som ansvarar för kontroller vid de yttre gränserna, vilka deltar i underrättelseförfarandet,

— kommissionsanställda såsom tjänstemän, tillfälligt anställda, kontraktsanställda, praktikanter och externa tjänsteleverantörer.

Följande uppgifter får behandlas:

— Förnamn på dem som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

— Efternamn på dem som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

— Namn på den myndighet som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

— Adress till den myndighet som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

— E-postadress till dem som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

— Telefonnummer till dem som har skrivit eller validerat anmälningar och reaktioner som lämnats in via Safety Gate-systemet.

c) Dessutom kan följande två typer av personuppgifter tillfälligtvis ingå i Safety Gate-systemet:

i) När det är nödvändigt för att spåra farliga produkter enligt definitionen i artikel 3.3 i förordning (EU) 2023/988 kan kontaktuppgifter till ekonomiska aktörer innehålla personuppgifter som kommer att ingå i Safety Gate-systemet. Sådana uppgifter förs in i Safety Gate-systemet endast av de nationella myndigheterna, på grundval av den information som samlats in under deras utredning. Följande uppgifter får behandlas:

— Ekonomiska aktörers namn.

— Ekonomiska aktörers adress.

— Ekonomiska aktörers ort.

— Ekonomiska aktörers land.

— Ekonomiska aktörers kontaktuppgifter ([1]).

([1]) Detta fält kan avse den fysiska person som företräder tillverkarna eller de auktoriserade representanterna. Medlemsstaterna uppmanas dock att undvika att föra in personuppgifter och att hellre använda kontaktuppgifter som inte är personliga, t.ex. generiska e-postadresser.

— Ekonomiska aktörers kontaktadress.

ii) Namn på personer som har utfört provningarna av farliga produkter och/eller bestyrkt provningsrapporterna, om de oavsiktligt har inkluderats i andra dokument, t.ex. provningsrapporter.

3.2 **Information till registrerade**

Kommissionen ska tillhandahålla den information som avses i artiklarna 15 och 16 och all kommunikation enligt artiklarna 17–24 och 35 i förordning (EU) 2018/1725 i en koncis, transparent, begriplig och lättillgänglig form med klart och tydligt språk. Kommissionen ska också vidta lämpliga åtgärder för att hjälpa de nationella myndigheterna att tillhandahålla information som avses i artiklarna 13 och 14 och kommunikation enligt artiklarna 19–26 och 37 i förordning (EU) 2016/679 i en koncis, transparent, begriplig och lättillgänglig form med klart och tydligt språk gällande följande uppgifter:

— Uppgifter som rör användare av Safety Gate-systemet.

— Uppgifter som rör dem som har skrivit och validerat anmälningar och reaktioner.

Användare av Safety Gate-systemet ska informeras om sina rättigheter genom det meddelande om skydd av personuppgifter som finns i Safety Gate-systemet.

De nationella myndigheterna ska vidta lämpliga åtgärder för att tillhandahålla information som avses i artiklarna 13 och 14 och kommunikation enligt artiklarna 19–26 och 37 i förordning (EU) 2016/679 i en koncis, transparent, begriplig och lättillgänglig form med klart och tydligt språk gällande följande uppgifter:

— Information om juridiska personer av vilken en fysisk persons identitet framgår.

— Namn på och andra uppgifter om personer som har utfört provningarna av farliga produkter och/eller bestyrkt provningsrapporterna.

Informationen ska tillhandahållas skriftligen, även elektroniskt.

När de nationella myndigheterna fullgör sina skyldigheter avseende registrerade ska de använda den mall för meddelande om skydd av personuppgifter vilken kommissionen har tillhandahållit.

3.3 **Hantering av begäranden från registrerade**

Registrerade får utöva sina rättigheter enligt förordning (EU) 2018/1725 eller förordning (EU) 2016/679 i förhållande till kommissionen respektive nationella myndigheter i egenskap av gemensamt personuppgiftsansvariga.

De gemensamt personuppgiftsansvariga ska hantera de registrerades begäranden i enlighet med det förfarande som de gemensamt personuppgiftsansvariga har fastställt för detta ändamål. Det detaljerade förfarandet för utövandet av de registrerades rättigheter förklaras i meddelandet om skydd av personuppgifter.

De gemensamt personuppgiftsansvariga ska samarbeta och på begäran ge varandra snabbt och effektivt bistånd vid hanteringen av registrerades begäranden.

Om en av de gemensamt personuppgiftsansvariga mottar en registrerads begäran som inte omfattas av dess ansvar ska den berörda gemensamt personuppgiftsansvariga omgående, och senast inom sju kalenderdagar från mottagandet, vidarebefordra begäran till den gemensamt personuppgiftsansvariga som faktiskt ansvarar för denna begäran. Den gemensamt personuppgiftsansvariga ska skicka ett mottagningsbevis till den registrerade inom tre kalenderdagar efter mottagandet av den vidarebefordrade begäran och samtidigt informera den gemensamt personuppgiftsansvariga som ursprungligen tog emot begäran om detta.

Som svar på en registrerads begäran om tillgång till personuppgifter får ingen gemensamt personuppgiftsansvarig lämna ut eller på annat sätt tillgängliggöra några personuppgifter som behandlats gemensamt utan att först samråda med den andra gemensamt personuppgiftsansvariga.

4. DE GEMENSAMT PERSONUPPGIFTSANSVARIGAS ANDRA ANSVAR OCH ROLLER

4.1 **Säkerhet vid behandling**

Varje gemensamt personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska åtgärder för att

a) trygga och skydda säkerheten, integriteten och konfidentialiteten för de personuppgifter som behandlas gemensamt, i enlighet med kommissionens beslut (EU, Euratom) 2017/46 ([2]) och respektive relevant rättsakt i EU-medlemsstaten eller Efta/EES-landet,

b) skydda mot obehörig eller olaglig behandling, förlust, användning, utlämnande eller förvärv av eller åtkomst till personuppgifter som den innehar,

c) inte lämna ut eller tillåta åtkomst till personuppgifter till någon annan än de på förhand överenskomna mottagarna eller personuppgiftsbiträdena.

Varje gemensamt personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska åtgärder för att trygga säkerheten vid behandling i enlighet med artikel 33 i förordning (EU) 2018/1725 respektive artikel 32 i förordning (EU) 2016/679.

De gemensamt personuppgiftsansvariga ska ge varandra snabbt och effektivt bistånd vid säkerhetsincidenter, inbegripet personuppgiftsincidenter.

4.2 **Hantering av säkerhetsincidenter, inbegripet personuppgiftsincidenter**

De gemensamt personuppgiftsansvariga ska hantera säkerhetsincidenter, inbegripet personuppgiftsincidenter, i enlighet med sina interna rutiner och tillämplig lagstiftning.

De gemensamt personuppgiftsansvariga ska i synnerhet förse varandra med snabbt och effektivt bistånd efter behov för att underlätta identifieringen och hanteringen av eventuella säkerhetsincidenter, däribland personuppgiftsincidenter, kopplade till den gemensamma behandlingen.

De gemensamt personuppgiftsansvariga ska underrätta varandra om följande:

a) Alla potentiella eller faktiska risker för tillgängligheten, konfidentialiteten och/eller integriteten för de personuppgifter som genomgår gemensam behandling.

b) Alla säkerhetsincidenter med koppling till den gemensamma behandlingen.

c) Alla personuppgiftsincidenter (dvs. varje säkerhetsöverträdelse som leder till oavsiktlig eller olaglig förstöring, förlust, ändring eller obehörig utlämning av eller obehörig åtkomst till de personuppgifter som genomgår gemensam behandling), de sannolika konsekvenserna av personuppgiftsincidenten och en bedömning av de risker fysiska personer utsätts för vad gäller deras rättigheter och friheter, samt alla åtgärder som har vidtagits för att åtgärda personuppgiftsincidenten och minska risken för fysiska personers rättigheter och friheter.

d) Alla överträdelser av de tekniska och/eller organisatoriska skyddsåtgärderna för den gemensamma behandlingen.

Varje gemensamt personuppgiftsansvarig ska vara ansvarig för att hantera alla säkerhetsincidenter, inbegripet personuppgiftsincidenter, som inträffar till följd av en överträdelse av den berörda gemensamt personuppgiftsansvarigas skyldigheter enligt denna genomförandeförordning samt förordning (EU) 2018/1725 respektive förordning (EU) 2016/679.

De gemensamt personuppgiftsansvariga ska dokumentera säkerhetsincidenter (inbegripet personuppgiftsincidenter) och underrätta varandra utan onödigt dröjsmål och senast inom 48 timmar efter att ha fått vetskap om en säkerhetsincident (inbegripet en personuppgiftsincident).

Den gemensamt personuppgiftsansvariga som är ansvarig för en personuppgiftsincident ska dokumentera den och underrätta Europeiska datatillsynsmannen eller den behöriga nationella tillsynsmyndigheten om personuppgiftsincidenten. Den ska göra detta utan onödigt dröjsmål och, om så är möjligt, senast 72 timmar efter att ha fått vetskap om personuppgiftsincidenten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Den ansvariga gemensamt personuppgiftsansvariga ska informera den andra gemensamt personuppgiftsansvariga om en sådan underrättelse.

Den gemensamt personuppgiftsansvariga som är ansvarig för personuppgiftsincidenten ska meddela de berörda registrerade om personuppgiftsincidenten om den sannolikt medför en hög risk för fysiska personers rättigheter och friheter. Den ansvariga gemensamt personuppgiftsansvariga ska informera den andra gemensamt personuppgiftsansvariga om ett sådant meddelande.

([2]) Kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem (EUT L 6, 11.1.2017, s. 40, ELI: http://data.europa.eu/eli/dec/2017/46/oj).

4.3 **Placering av personuppgifter**

Personuppgifter som samlas in för underrättelseprocessen genom Safety Gate-systemet ska lagras och samlas i Safety Gate-systemet i syfte att säkerställa att åtkomsten till applikationen begränsas till klart identifierade personer och därmed att de uppgifter som lagras i applikationen är väl skyddade.

Personuppgifter som samlas in för behandlingen får endast behandlas inom EU:s/EES territorium och får inte lämna det territoriet, såvida de inte är förenliga med artikel 45, 46 eller 49 i förordning (EU) 2016/679 eller artikel 47, 48 eller 50 i förordning (EU) 2018/1725.

Enligt artikel 40 i förordning (EU) 2023/988 får kommissionen förse tredjeländer eller internationella organisationer med utvald information från Safety Gate-systemet och få relevant information om produkters säkerhet och om förebyggande, begränsande och korrigerande åtgärder som vidtagits av dessa tredjeländer eller internationella organisationer. Informationsutbyte enligt artikel 40 i förordning (EU) 2023/988 ska, i den mån det rör sig om personuppgifter, ske i enlighet med unionens dataskyddsregler.

4.4 Mottagare av personuppgifter

Åtkomst till personuppgifter ska endast beviljas bemyndigad personal och bemyndigade uppdragstagare vid kommissionen och nationella myndigheter i syfte att administrera och driva Safety Gate-systemet. Denna åtkomst ska omfattas av följande identitets- och lösenordskrav:

— Safety Gate-systemet ska endast vara öppet för kommissionen och för användare som specifikt utsetts av EU-medlemsstaternas myndigheter och av myndigheter i Efta-/EES-länder samt i Förenade kungariket med avseende på användare i Nordirland.

— Åtkomst till de insamlade personuppgifterna i Safety Gate-systemet ska endast beviljas de utsedda och behöriga användare av applikationen som har ett användar-id/lösenord. Åtkomst till applikationen och beviljande av lösenord ska endast vara möjligt om detta begärs av den behöriga nationella myndigheten under allmän tillsyn av kommissionens Safety Gate-grupp.

— Åtkomst till de insamlade personuppgifterna ska ges till den kommissionspersonal som ansvarar för denna behandling och till behöriga personer i enlighet med principen om behovsenlig behörighet. Personalen är bunden av sekretessregler och vid behov ytterligare överenskommelser om sekretess.

Följande personer ska ha åtkomst till de insamlade personuppgifterna:

a) Kommissionens personal och uppdragstagare.

b) Angivna kontaktpunkter och inspektörer från marknadskontrollmyndigheterna i EU:s medlemsstater och Efta-/EES-länderna samt brittiska myndigheter med avseende på användare i Nordirland.

c) Angivna inspektörer från de myndigheter som ansvarar för kontroller vid de yttre gränserna i EU:s medlemsstater och Efta-/EES-länderna.

Följande personer ska ha åtkomst till alla insamlade personuppgifter och ha möjlighet att på begäran ändra dem:

a) Medlemmar i kommissionens Safety Gate-grupp.

b) Medlemmar i kommissionens Safety Gate-helpdesk.

En förteckning över alla Safety Gate-kontaktpunkter, med kontaktuppgifter (efternamn, förnamn, myndighetens namn och adress, telefonnummer, e-postadress) ska finnas tillgänglig på Safety Gate-portalen ([3]). Användarhanteringen på nationell nivå ska kontrolleras av Safety Gate-kontaktpunkterna genom Safety Gate-systemet.

([3]) https://ec.europa.eu/safety-gate/#/screen/pages/contacts.

Alla användare ska ha åtkomst till innehållet i anmälningar med status som ”EC validated” (validerad av kommissionen). Endast nationella användare av Safety Gate-systemet ska ha åtkomst till utkastet till sina anmälningar (innan de lämnas till kommissionen). Kommissionens personal och behöriga personer ska ha åtkomst till anmälningar med status som ”inlämnad till kommissionen”.

Varje gemensamt personuppgiftsansvarig ska informera alla andra gemensamt personuppgiftsansvariga om eventuella överföringar av personuppgifter till mottagare i tredjeländer eller internationella organisationer.

5. DE GEMENSAMT PERSONUPPGIFTSANSVARIGAS SPECIFIKA ANSVARSOMRÅDEN

Kommissionen ska säkerställa och ansvara för att göra följande:

a) Besluta om medel, krav och ändamål för behandlingen.

b) Registrera behandlingen.

c) Göra det lättare för de registrerade att utöva sina rättigheter.

d) Hantera begäranden från registrerade.

e) Besluta om att begränsa tillämpningen av eller göra undantag från registrerades rättigheter, när detta är nödvändigt och proportionellt.

f) Säkerställa inbyggt integritetsskydd och integritetsskydd som standard.

g) Identifiera och bedöma om översändningar och överföringar av personuppgifter är lagliga, nödvändiga och proportionella.

h) Vid behov samråda på förhand med Europeiska datatillsynsmannen.

i) Säkerställa att personer med behörighet att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

j) På begäran samarbeta med Europeiska datatillsynsmannen vid utförandet av dennas uppgifter.

De nationella myndigheterna ska säkerställa och ansvara för att göra följande:

a) Registrera behandlingen.

b) Säkerställa att de personuppgifter som genomgår behandling är adekvata, korrekta, relevanta och begränsade till vad som är nödvändigt för ändamålet.

c) Säkerställa transparent information och kommunikation till de registrerade om deras rättigheter.

d) Göra det lättare för de registrerade att utöva sina rättigheter.

e) Använda enbart personuppgiftsbiträden som ger tillräckliga garantier för att vidta lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordning (EU) 2016/679 och tryggar skyddet av registrerades rättigheter.

f) Reglera personuppgiftsbiträdets behandling genom ett avtal eller en rättsakt enligt unionsrätten eller enligt medlemsstatens nationella rätt i enlighet med artikel 28 i förordning (EU) 2016/679.

g) Vid behov samråda på förhand med sin nationella tillsynsmyndighet.

h) Säkerställa att personer med behörighet att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

i) På begäran samarbeta med sin nationella tillsynsmyndighet vid utförandet av dess uppgifter.

6. BEHANDLINGENS VARAKTIGHET

Gemensamt personuppgiftsansvariga får inte lagra eller behandla personuppgifter längre än vad som är nödvändigt för att fullgöra de överenskomna ändamålen och skyldigheterna i enlighet med denna förordning, dvs. under den tid som krävs för att uppfylla ändamålet med insamlingen eller vidarebehandlingen. I synnerhet gäller följande:

a) Kontaktuppgifter för användarna av Safety Gate-systemet ska bevaras i systemet så länge de är användare. Kontaktuppgifterna ska raderas från Safety Gate-systemet omedelbart efter mottagandet av information om att en viss person inte längre är användare av systemet.

b) Kontaktuppgifter till inspektörerna från marknadskontrollmyndigheterna i medlemsstaterna och Efta-/EES-länderna, liksom inspektörerna från de myndigheter som ansvarar för kontroller vid de yttre gränserna, i anmälningar och reaktioner ska bevaras i systemet i fem år efter valideringen av anmälan eller reaktionen.

c) Personuppgifter om andra fysiska personer som eventuellt finns i systemet ska bevaras i en form som möjliggör identifiering i 30 år från den tidpunkt då informationen matas in i Safety Gate-systemet, vilket motsvarar den uppskattade maximala livscykeln för produktkategorier såsom elektriska apparater eller motorfordon.

Berättigade begäranden från registrerade om att få sina uppgifter blockerade, justerade eller raderade ska tillmötesgås av kommissionen inom en månad från mottagandet av begäran.

7. ANSVAR FÖR BRISTANDE EFTERLEVNAD

Kommissionen ska ha ansvar för bristande efterlevnad i enlighet med kapitel VIII i förordning (EU) 2018/1725.

EU-medlemsstaternas myndigheter ska ha ansvar för bristande efterlevnad i enlighet med kapitel VIII i förordning (EU) 2016/679.

8. SAMARBETE MELLAN GEMENSAMT PERSONUPPGIFTSANSVARIGA

Varje gemensamt personuppgiftsansvarig ska på begäran ge snabbt och effektivt bistånd till de andra gemensamt personuppgiftsansvariga vid tillämpningen av denna förordning, samtidigt som den följer alla tillämpliga krav i förordningarna (EU) 2018/1725 respektive (EU) 2016/679, och andra tillämpliga dataskyddsregler.

9. TVISTLÖSNING

De gemensamt personuppgiftsansvariga ska sträva efter att i godo lösa eventuella tvister som uppstår till följd av eller som rör tolkningen eller tillämpningen av denna förordning.

Om det vid någon tidpunkt uppstår frågor, tvister eller meningsskiljaktigheter mellan de gemensamt personuppgiftsansvariga med avseende på eller i samband med denna förordning ska de gemensamt personuppgiftsansvariga göra sitt yttersta för att lösa dessa genom samråd.

Helst ska alla tvister lösas på operativ nivå allteftersom de uppstår och lösas av de kontaktpunkter som avses i punkt 10 i denna bilaga och förtecknas på Safety Gate-portalen.

Ändamålet med samrådet ska vara att se över och i praktiskt möjligaste mån komma överens om vilka åtgärder som ska vidtas för att lösa problemet. De gemensamt personuppgiftsansvariga ska i detta syfte förhandla med varandra i god tro. Varje gemensamt personuppgiftsansvarig ska besvara en begäran om uppgörelse i godo inom sju arbetsdagar efter mottagandet av en sådan begäran. En uppgörelse i godo ska uppnås inom 30 arbetsdagar från och med den dag då begäran mottogs.

Om tvisten inte kan lösas i godo får varje gemensamt personuppgiftsansvarig söka medling och/eller rättsliga förfaranden på följande sätt:

a) När det gäller medling ska de gemensamt personuppgiftsansvariga tillsammans utse en medlare som var och en av dem kan godta och som ska ansvara för att främja lösningen av tvisten inom två månader efter att tvisten har hänskjutits till denna.

b) När det gäller rättsliga förfaranden ska ärendet hänskjutas till Europeiska unionens domstol i enlighet med artikel 272 i fördraget om Europeiska unionens funktionssätt.

10. KONTAKTPUNKTER FÖR SAMARBETE MELLAN DE GEMENSAMT PERSONUPPGIFTSANSVARIGA

Varje gemensamt personuppgiftsansvarig utser en enda kontaktpunkt, som andra gemensamt personuppgiftsansvariga ska kontakta vid frågor, klagomål och tillhandahållande av information inom ramen för denna förordning.

En detaljerad förteckning över alla kontaktpunkter som utsetts av kommissionen och de nationella myndigheterna, med kontaktuppgifter (efternamn, förnamn, myndighetens namn och adress, telefonnummer, fax, e-postadress) ska finnas tillgänglig på Safety Gate-portalen.