Behandling av personuppgifter i Transport- och kommunikationsverkets NIS2-rapporteringssystem

Personuppgiftsansvarig Transport- och kommunikationsverket (Traficom)	**Kontaktuppgifter till den personuppgiftsansvarige** PB 320, 00059 TRAFICOM registrator@traficom.fi telefon 029 534 5000 **Kontaktuppgifter till den personuppgiftsansvariges dataskyddsombud** PB 320, 00059 TRAFICOM tietosuoja@traficom.fi telefon 029 534 5000 Om ditt meddelande innehåller känsligt, sekretessbelagt eller annars sensitivt innehåll eller en personbeteckning, ber vi dig att använda Traficoms säkra e-post.

Grunden för och ändamålet med behandlingen av uppgifter

Behandlingen av personuppgifter grundar sig på fullgörande av en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c i den allmänna dataskyddsförordningen (EU) (2016/679)).

Enligt 11 § i cybersäkerhetslagen (124/2025) ska en aktör (som enligt 26 § i cybersäkerhetslagen och 18 h § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) omfattar Transport- och kommunikationsverket, Energimyndigheten, Säkerhets- och kemikalieverket, Tillstånds- och tillsynsverket för social- och hälsovården, Närings-, trafik- och miljöcentralen i Södra Savolax, Livsmedelsverket samt Säkerhets- och utvecklingscentret för läkemedelsområdet) utan dröjsmål underrätta tillsynsmyndigheten om en betydande incident. Med en betydande incident avses en incident som har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för den berörda aktören, samt en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. Den första anmälan ska göras inom 24 timmar från det att den betydande incidenten upptäcktes och den uppföljande anmälan inom 72 timmar från det att den betydande incidenten upptäcktes. I den första anmälan ska uppges 1) att en betydande incident har upptäckts, 2) om den betydande incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar, 3) möjligheten och sannolikheten för gränsöverskridande verkningar och uppgifter om förväntad utveckling vad gäller gränsöverskridande verkningar. I den uppföljande anmälan ska uppges 1) en bedömning av den betydande incidentens art, allvarlighetsgrad och konsekvenser, 2) i förekommande fall, tekniska angreppsindikatorer, 3) eventuella uppdateringar av uppgifterna i den första anmälan.

Enligt 12 § i cybersäkerhetslagen ska aktören på begäran av tillsynsmyndigheten lämna ytterligare information eller en delrapport om statusuppdateringar som gäller den betydande incidenten och om hur hanteringen framskrider.

Enligt 13 § i cybersäkerhetslagen ska aktören lämna tillsynsmyndigheten en slutrapport om en betydande incident inom en månad från det att den uppföljande anmälan lämnades in eller, om det är fråga om en långvarig incident, inom en månad från det att hanteringen av

den avslutades. Slutrapporten ska innehålla 1) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser, 2) en redogörelse för den typ av hot eller grundorsak som sannolikt har utlöst incidenten, 3) en redogörelse för tillämpade och pågående åtgärder för att begränsa konsekvenserna av incidenten, och 4) en redogörelse för eventuella gränsöverskridande konsekvenser. Offentliga förvaltningsentiteters skyldighet att anmäla betydande incidenter regleras i 18 d § i lagen om informationshantering inom den offentliga förvaltningen

Enligt 15 § 1 mom. i cybersäkerhetslagen kan aktörer på frivillig basis underrätta tillsynsmyndigheten om andra än i 11 § avsedda incidenter, cyberhot och tillbud. Enligt 15 § 2 punkten i cybersäkerhetslagen ska tillsynsmyndigheten informera den i 18 § avsedda gemensamma kontaktpunkten om underrättelser enligt denna paragraf. Offentliga förvaltningsentiteters möjlighet till frivillig underrättelse regleras i 18 f § i lagen om informationshantering inom den offentliga förvaltningen

Enligt 17 § i cybersäkerhetslagen ska tillsynsmyndigheten omedelbart lämna de anmälningar, underrättelser och rapporter som avses i 11–13 och 15 § till CSIRT-enheten. Om en betydande incident påverkar en annan medlemsstat i Europeiska unionen ska den gemensamma kontaktpunkten utan onödigt dröjsmål underrätta Europeiska unionens cybersäkerhetsbyrå och de medlemsstater som berörs av incidenten. Den gemensamma kontaktpunkten ska på begäran också sända de anmälningar och rapporter som avses i 11–13 § till den gemensamma kontaktpunkten i den medlemsstat som berörs av incidenten. Den gemensamma kontaktpunkten får i detta syfte lämna ut information om betydande incidenter till Europeiska unionens cybersäkerhetsbyrå och till de gemensamma kontaktpunkterna i andra medlemsstater i Europeiska unionen. För offentlig förvaltningsentitet, se 18 h § i lagen om informationshantering inom den offentliga förvaltningen.

Enligt 18 § i cybersäkerhetslagen är Cybersäkerhetscentret vid Transport- och kommunikationsverket den gemensamma kontaktpunkt som avses i artikel 8.3 i NIS 2-direktivet. Den gemensamma kontaktpunkten har till uppgift att främja samarbetet och samordningen mellan tillsynsmyndigheterna vid fullgörandet av uppgifter enligt denna lag. Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Europeiska unionens cybersäkerhetsbyrå med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilka det har underrättats med stöd av 11–13 och 15 §. Den gemensamma kontaktpunkten har rätt att för detta ändamål få anonymiserade och aggregerade uppgifter av tillsynsmyndigheten. För offentlig förvaltningsentitet, se 18 h § i lagen om informationshantering inom den offentliga förvaltningen.

För dessa ändamål samlas information genom Transport- och kommunikationsverkets applikation för NIS2-rapporter om de betydande incidenter (obligatorisk rapport) som aktörer rapporterat samt om frivilliga rapporter. För att kunna genomföra insamlingen av denna information är det nödvändigt att behandla personuppgifter som beskrivs i denna dataskyddsbeskrivning.

Datainnehåll	
Informationsmaterial som behandlas	I registret behandlas aktörernas uppgifter om betydande cybersäkerhetsincidenter enligt rapporterna. Dessa uppgifter kan innehålla personuppgifter. De registrerade är den som lämnat rapporten samt de personer vars uppgifter anges på blanketten.

	Personuppgifter som behandlas är uppgifter om de personer som informationssäkerhetsincidenten gäller som har angetts i meddelanden till den personuppgiftsansvarige eller i blankettens öppna fält samt bilagor, som till exempel: 1) Kontaktuppgifter såsom namn, e-post, telefonnummer, adress, roll i organisationen samt andra kontaktuppgifter som angetts; 2) Uppgifter om incidenten och personuppgifter i anslutning till dem, 3) Tekniska uppgifter angående anmälaren, såsom IP-adress, uppgift om webbläsare och webbläsarversion, 4) Andra (även särskilda) uppgifter om den registrerade som eventuellt framgår av beskrivningen av cybersäkerhetsincidenten eller personbeteckning (till exempel vid nätfiske) samt uppgifter som kan härledas från personbeteckningen såsom ålder och kön. Den eventuella behandlingen av särskilda kategorier av personuppgifter grundar sig på artikel 9.2 g samt eventuellt artikel 9.2 e i den allmänna dataskyddsförordningen (EU). Eventuell behandling av personbeteckning sker på basis av 29 § 1 mom. i dataskyddslagen.
Informationskällor för informationsinnehållet som behandlas (varifrån uppgifter erhålls)	Uppgifterna som behandlas erhålls från anmälaren. Uppgifterna lämnas på en blankett som finns på Cybersäkerhetscentrets webbplats. Uppgifter kan också fås från kommunikationen som gäller incidenten mellan den personuppgiftsansvarige och den som fyllt i anmälningsblanketten eller någon annan kontaktperson.
Lagringstiden för personuppgifter	Personuppgifterna lagras så länge som behandlingen är nödvändig för att uppfylla ändamålen som beskrivs i denna dataskyddsbeskrivning, dock högst i sex år efter utgången av det kalenderår under vilket informationen erhölls.

Behandling av uppgifter	
Mottagarna och de kategorier av mottagare som ska ta del av personuppgifterna (till vem uppgifter lämnas ut)	Incidentinformation, inklusive personuppgifter, förmedlas via applikationen till myndigheten som övervakar aktören i fråga samt till CSIRT och den gemensamma kontaktpunkten. Uppgifterna lämnas inte ut till direktmarknadsföring.
Behandling av personuppgifter för den personuppgiftsansvariges räkning	Det finns inga separata personuppgiftsbiträden, personuppgifter behandlas alltså inte för den personuppgiftsansvariges räkning.
Överföring av personuppgifter till tredjeländer utanför EU/EES	Personuppgifter överförs inte utanför EU/EES.
Automatiserat beslutsfattande och profilering	Automatiserat beslutsfattande eller profilering används inte.

Rättigheter i samband med behandling av personuppgifter

Om utövande av rättigheter

Du kan utöva dina rättigheter genom att skicka en begäran till Traficom per e-post eller post. Kontaktuppgifterna finns i punkten ”Kontaktuppgifter till den personuppgiftsansvarige” i dataskyddsbeskrivningen.

Rätt att lämna in klagomål till tillsynsmyndigheten

Om du anser att behandlingen av dina personuppgifter strider mot lagstiftningen, kan du lämna in ett klagomål till Dataombudsmannens byrå.

Dataombudsmannens byrå
PB 800, 00531 Helsingfors
tietosuoja(at)om.fi
tfn 029566 6700

Rätt att få tillgång till uppgifter om sig själv	Den registrerade har rätt att av den personuppgiftsansvarige få en bekräftelse på att personuppgifter om honom eller henne behandlas eller inte behandlas och om de behandlas, rätt att få tillgång till personuppgifterna.
Rätt till rättelse	Den registrerade har rätt att kräva att den personuppgiftsansvarige utan obefogat dröjsmål rättar inexakta och felaktiga personuppgifter om den registrerade.
Rätt att göra invändningar	Eftersom behandlingsgrunden är fullgörande av en rättslig förpliktelse har den registrerade inte rätt att göra invändningar.
Rätt att begränsa behandlingen av uppgifter	Den registrerade har rätt att kräva att den personuppgiftsansvarige begränsar behandlingen om - den registrerade bestrider personuppgifternas riktighet - behandlingen är olaglig, men den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning - den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen, men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk - den registrerade har invänt mot behandling av personuppgifter i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.
Rätt till dataportabilitet	Den registrerade har rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som personuppgifterna tillhandahållits till hindrar detta, om behandlingen av personuppgifter grundar sig på samtycke eller avtal och behandlingen sker automatiserat.
Rätt till radering	I de situationer där behandlingen av personuppgifterna baserar sig på en annan rättsgrund än fullgörandet av en rättslig förpliktelse har den registrerade rätt att begära att personuppgifterna raderas. De begärda uppgifterna raderas om den personuppgiftsansvarige inte har

	någon lagenlig grund att neka till raderingen, såsom en lagstadgad skyldighet att lagra uppgifterna.
Rätt att återkalla samtycke	