Exempel på personuppgiftsincidenter och vem som ska underrättas

Följande icke-uttömmande förteckning kommer att hjälpa personuppgiftsansvariga att avgöra huruvida de behöver anmäla en personuppgiftsincident i olika situationer. Exemplen kan även göra det lättare att skilja mellan risk och hög risk för enskilda personers rättigheter och friheter.

Exempel	**Anmäla till tillsyns-myndigheten?**	**Underrätta den registrerade?**	**Anmärkningar/ rekommendationer**
i. En personuppgifts-ansvarig sparade en säkerhetskopia av ett arkiv över personuppgifter på ett USB-minne. Minnet stals under ett inbrott.	Nej.	Nej.	Så länge uppgifterna är krypterade med den senaste typen av algoritm, det finns säkerhetskopior av uppgifterna, det unika minnet inte har äventyrats och uppgifterna snabbt kan återställas, är det inte säkert att incidenten behöver rapporteras. Om uppgifterna senare äventyras krävs dock en anmälan.
ii. En personuppgifts-ansvarig driver en onlinetjänst. Till följd av ett it-angrepp på den tjänsten har enskilda personers personuppgifter exfiltrerats. Den personuppgifts-ansvarige har kunder i en enda medlemsstat.	Ja, rapportera till tillsynsmyndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer.	Ja, rapportera till enskilda personer beroende på de berörda person-uppgifternas art och om det är sannolikt att de leder till mycket allvarliga konsekvenser för enskilda personer.	
iii. Ett kort strömavbrott under några minuter på en personuppgiftsansvarigs teletjänstcentral innebär att kunder inte kan ringa till den personuppgifts-	Nej.	Nej.	Detta är inte en incident som behöver anmälas, men som trots det ska registreras enligt artikel 33.5.

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

Gruppens sekretariatet finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) på Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, kontor MO-59 02/013.

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

ansvarige och få tillgång till sina uppgifter.			Den personuppgifts-ansvarige bör föra ett lämpligt register.
iv. En personuppgifts-ansvarig utsätts för ett angrepp med ransomware vilket leder till att alla uppgifter krypteras. Det finns inga säkerhetskopior och uppgifterna kan inte återställas. Vid en närmare undersökning visar det sig att det enda syftet med angreppet var att kryptera uppgifterna, och att det inte fanns några andra sabotageprogram i systemet.	Ja, rapportera till tillsynsmyndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer eftersom detta utgör en förlust av tillgänglighet.	Ja, rapportera till enskilda personer, beroende på de berörda person-uppgifternas art och de potentiella konsekvenserna av förlusten av tillgänglighet, samt andra sannolika konsekvenser.	Om det fanns en säkerhetskopia och uppgifterna snabbt kunde återställas behöver incidenten inte rapporteras till tillsynsmyndigheten eller till de enskilda personerna eftersom det inte har varit tal om någon permanent förlust av tillgänglighet eller konfidentialitet. Om tillsynsmyndig-heten emellertid fick vetskap om incidenten på annat sätt kan den överväga att göra en undersökning för att bedöma efterlevnaden av de mer allmänna säkerhetskraven i artikel 32.
v. En person ringer en banks teletjänstcentral för att rapportera en personuppgiftsincident. Personen har fått någon annans månatliga kontoutdrag. Den personuppgifts-ansvarige genomför en kort undersökning (som slutförs inom 24 timmar) och fastställer med rimlig säkerhet att en person-uppgiftsincident har ägt rum och huruvida det finns en brist i systemet som innebär att andra personer har påverkats eller kan påverkas.	Ja.	Endast de personer som påverkades underrättas om det finns en hög risk och det är uppenbart att andra personer inte påverkades.	Om det efter en närmare undersökning visar sig att fler personer påverkas måste en uppdatering göras till tillsyns-myndigheten, och den personuppgifts-ansvarige ska vidta de ytterligare åtgärder som krävs genom att underrätta andra personer om det finns en hög risk för dem.
vi. En personuppgifts-ansvarig driver en marknadsplats på nätet och har kunder i flera medlemsstater. Marknadsplatsen utsätts för ett it-angrepp och angriparen publicerar	Ja, rapportera till ansvarig tillsyns-myndighet om det rör sig om gränsöverskridande behandling.	Ja, eftersom detta kan leda till en hög risk.	Den personuppgifts-ansvarige bör vidta åtgärder, t.ex. att tvinga de berörda kontona att återställa lösenorden och andra åtgärder för att minska risken.

användarnamn, lösenord och köphistorik på nätet.			Den personuppgifts-ansvarige bör även överväga andra anmälningsskyldigheter t.ex. enligt NIS-direktivet som leverantör av digitala tjänster.
vii. Ett webbhotell som fungerar som person-uppgiftsbiträde noterar ett fel i den kod som styr användarauktorisationen. Konsekvensen av bristen innebär att alla användare kan få tillgång till alla andra användares kontouppgifter.	Som personuppgifts-biträde måste webb-hotellet underrätta de berörda kunderna (de personuppgiftsan-svariga) utan onödigt dröjsmål. Förutsatt att webb-hotellet har gjort en egen undersökning bör de berörda personupp-giftsansvariga vara rimligen säkra på huruvida de har drabbats av en incident, och därför ska anses ha ”fått vetskap”, så snart de har underrättats av webbhotellet (person-uppgiftsbiträdet). Den personuppgiftsansvarige ska därefter underrätta tillsynsmyndigheten.	Om det sannolikt inte finns någon hög risk för enskilda personer behöver dessa inte underrättas.	Webbhotellet (person-uppgiftsbiträdet) måste överväga andra an-mälningsskyldigheter (t.ex. enligt NIS-direktivet som leverantör av digitala tjänster). Om det inte finns något som tyder på att denna sårbarhet har utnyttjats av någon av de personuppgifts-ansvariga är det inte säkert att incidenten behöver anmälas men den måste sannolikt registreras som ett exempel på bristande efterlevnad enligt artikel 32.
viii. Patientjournaler på ett sjukhus är inte tillgängliga under 30 dagar på grund av ett it-angrepp.	Ja, sjukhuset är skyldigt att anmäla incidenten eftersom den kan leda till hög risk för patienternas välbefinnande och deras personliga integritet.	Ja, rapportera till de personer som påverkas.	
ix. Personuppgifter från en stor mängd studenter skickas av misstag till fel sändlista med över 1 000 mottagare.	Ja, rapportera till tillsynsmyndigheten.	Ja, rapportera till enskilda personer beroende på de berörda person-uppgifternas omfattning och typ och de potentiella konsekvensernas svårighetsgrad.	
x. Ett e-postmeddelande i direktmarknadsföringssyfte skickas till mottagare i	Ja, det kan vara obligatoriskt att anmäla incidenten till	Ja, rapportera till enskilda personer	En anmälan är eventuellt inte nödvändig om ingen

fälten ”till:” eller ”cc:”, vilket gör det möjligt för alla mottagare att se andra mottagares e-postadress.	tillsynsmyndigheten om en stor mängd personer berörs, om känsliga uppgifter röjs (t.ex. en psykoterapeuts sändlista) eller om andra faktorer innebär en hög risk (t.ex. att e-postmeddelandet innehåller de ursprungliga lösenorden).	beroende på de berörda personuppgifternas omfattning och typ och de potentiella konsekvensernas svårighetsgrad.	känslig information röjs och endast ett litet antal e-postadresser har avslöjats.