AUTORITEIT
PERSOONSGEGEVENS

Voorbeeldlijst wel/niet melden datalek

Heeft uw organisatie een datalek? Dan kan het zijn dat u dit moet melden aan de Autoriteit Persoonsgegevens (AP) en aan de betrokken personen. Dit hangt af van het risico op schade. U moet dit zelf inschatten. De voorbeelden in dit overzicht kunt u gebruiken als hulpmiddel. In het dossier 'Meldplicht datalekken' op onze website vindt u meer informatie over het beoordelen van de risico's.

VOORBEELD	MELDEN AAN AP	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een verwerkingsverantwoordelijke heeft een back-up van een archief van persoonsgegevens op een USB-stick opgeslagen. De USB-stick wordt gestolen tijdens een inbraak.	NEE	NEE	Zolang de gegevens met een geavanceerd algoritme zijn versleuteld, er back-ups van de gegevens bestaan, de unieke sleutel niet is gecompromitteerd en de gegevens tijdig kunnen worden hersteld, is het mogelijk dat deze inbreuk niet hoeft te worden gemeld. Vindt er later echter een compromittering plaats, moet de inbreuk wel worden gemeld.
Een verwerkingsverantwoordelijke exploiteert een online dienst. Als gevolg van een cyberaanval op die dienst worden persoonsgegevens geëxtraheerd. De verwerkingsverantwoordelijke heeft klanten in een enkele lidstaat.	JA Meld deze inbreuk aan de toezichthoudende autoriteit als er waarschijnlijk gevolgen zijn voor personen.	JA Deel deze inbreuk mee aan personen afhankelijk van de aard van de betrokken persoonsgegevens en of de waarschijnlijke gevolgen voor personen zeer ernstig zijn.	

Deze voorbeelden zijn gebaseerd op de voorbeeldlijst uit de 'Guidelines voor melding van inbreuken in verband met persoonsgegevens', opgesteld door de Europese privacytoezichthouders.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een stroomstoring van enkele minuten in het callcenter van een verwerkingsverantwoordelijke heeft tot gevolg dat klanten de verwerkings-verantwoordelijke niet kunnen bellen en geen toegang hebben tot hun gegevens.	NEE	NEE	Dit is geen te melden inbreuk, maar wel een te registreren incident overeenkomst artikel 33, lid 5. De verwerkingsverantwoordelijke dient de nodige gegevens te registreren en bij te houden.
Een verwerkingsverantwoordelijke wordt het slachtoffer van een ransomware-aanval. Het gevolg is dat al zijn gegevens zijn versleuteld. Er zijn geen back-ups beschikbaar en de gegevens kunnen niet worden hersteld. Tijdens het onderzoek wordt duidelijk dat de enige functionaliteit van de ransomware het versleutelen van de gegevens was en dat er geen andere malware in het systeem aanwezig was.	JA Meld deze inbreuk aan de toezichthoudende autoriteit als er waarschijnlijk gevolgen zijn voor personen, aangezien dit een verlies van beschikbaarheid is.	JA Deel deze inbreuk mee aan personen afhankelijk van de aard van de betrokken persoonsgegevens en de mogelijke gevolgen van het niet beschikbaar zijn van de gegevens, alsmede andere waarschijnlijke gevolgen.	Als een back-up beschikbaar was en de gegevens tijdig konden worden hersteld, moest deze inbreuk niet aan de toezichthoudende autoriteit worden gemeld noch aan personen worden meegedeeld aangezien er geen permanent verlies van beschikbaarheid of vertrouwelijkheid zou zijn geweest. Als de toezichthoudende autoriteit echter op een andere wijze kennis heeft gekregen van het incident, kan zij een onderzoek overwegen om na te gaan of aan de ruimere veiligheidseisen van artikel 32 is voldaan.
Een persoon belt naar het callcenter van een bank om een inbreuk in verband met persoonsgegevens te melden. De persoon heeft een maandoverzicht van iemand anders ontvangen. De verwerkingsverantwoordelijke voert een kort onderzoek uit (het onderzoek wordt binnen de 24 uur afgerond) en stelt met een redelijke mate van zekerheid vast dat er zich een inbreuk in verband met persoonsgegevens heeft voorgedaan. Hij vraagt zich af of er zich ergens een systeemstoring voordoet, in welk geval dit mogelijk gevolgen heeft gehad of zou kunnen hebben voor andere personen.	JA	De inbreuk wordt alleen meegedeeld aan de getroffen personen als er een hoog risico is en het duidelijk is dat anderen niet zijn getroffen.	Indien na nader onderzoek wordt vastgesteld dat er meer personen getroffen zijn, moet de toezichthoudende autoriteit hiervan in kennis worden gesteld en moet de verwerkingsverant-woordelijke de inbreuk meedelen aan andere personen indien er een groot risico voor hen bestaat.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Een verwerkingsverantwoordelijke exploiteert een onlinemarktplaats en heeft klanten in meerdere lidstaten. De marktplaats wordt getroffen door een cyberaanval, en de aanvaller publiceert gebruikersnamen, wachtwoorden en aankoopoverzichten op het internet.	JA Meld de inbreuk aan de leidende toezichthoudende autoriteit als het gaat om grensoverschrijdende verwerking.	JA Aangezien dit tot een groot risico zou kunnen leiden.	De verwerkingsverantwoordelijke dient actie te ondernemen, bijvoorbeeld door de getroffen accounts te verplichten hun wachtwoorden te wijzigen, evenals andere stappen om het risico te beperken. De verwerkingsverantwoordelijke dient ook andere kennisgevingsverplichtingen in overweging te nemen, bijvoorbeeld op grond van de NIS-richtlijn als digitale dienstverlener.
Een als gegevensverwerker optredend hostingbedrijf constateert een fout in de code voor de autorisatie van gebruikers. Het gevolg van de fout is dat elke gebruiker toegang kan krijgen tot de accountgegevens van elke andere gebruiker.	Als verwerker moet het hostingbedrijf zijn getroffen klanten (de verwerkingsverantwoordelijken) onverwijld hiervan in kennis stellen. In de veronderstelling dat het hostingbedrijf zijn eigen onderzoek heeft verricht, zouden de getroffen verwerkingsverantwoordelijken redelijke zekerheid moeten hebben over de vraag of ze het slachtoffer zijn geworden van een inbreuk. Bijgevolg wordt het waarschijnlijk geacht dat ze "kennis" hebben gekregen van de inbreuk zodra ze door het hostingbedrijf (de verwerker) daarvan in kennis zijn gesteld. De verwerkings-verantwoordelijke dient de inbreuk vervolgens te melden aan de toezichthoudende autoriteit.	Als er waarschijnlijk geen hoog risico voor de personen is, moet de inbreuk niet aan hen worden meegedeeld.	Het hostingbedrijf (verwerker) moet alle andere kennisgevingsverplichtingen (bijvoorbeeld op grond van de NIS-richtlijn als een digitale dienstverlener) in overweging nemen. Als er geen aanwijzingen zijn dat er bij een van de verwerkingsverantwoordelijken misbruik wordt gemaakt van deze kwetsbaarheid, is er mogelijk geen sprake van een te melden inbreuk. Wel zal deze inbreuk waarschijnlijk moeten worden geregistreerd of worden beschouwd als een geval van niet-naleving overeenkomstig artikel 32.

VOORBEELD	MELDEN AAN AP*	MEEDELEN AAN BETROKKENEN?	OPMERKINGEN / AANBEVELINGEN
Als gevolg van een cyberaanval zijn de medische dossiers in een ziekenhuis gedurende 30 uur niet beschikbaar.	JA Het ziekenhuis is verplicht om te melden dat de inbreuk een hoog risico kan inhouden voor het welzijn en de patiënt	JA Deel deze inbreuk mee aan de getroffen personen.	
Persoonsgegevens van een groot aantal studenten worden per ongeluk naar de verkeerde mailinglijst gestuurd ... een lijst met meer dan 1 000 ontvangers.	JA Meld deze inbreuk aan de toezichthoudende autoriteit.	JA Deel deze inbreuk mee aan personen, afhankelijk van de omvang en het type persoonsgegevens en de ernst van de mogelijke gevolgen.	
Een direct-marketingmail wordt verzonden naar ontvangers in het veld "Aan" of "CC", waardoor elke ontvanger het e-mailadres van de andere ontvangers kan zien.	JA Het kan verplicht zijn om deze inbreuk te melden aan de toezichthoudende autoriteit als een groot aantal personen erdoor getroffen is, als er gevoelige gegevens zijn onthuld (bijvoorbeeld een mailinglijst van een psychotherapeut) of als andere factoren hoge risico's inhouden (bijvoorbeeld als de mail de oorspronkelijke wachtwoorden bevat).	JA Deel deze inbreuk mee aan personen, afhankelijk van de omvang en het type persoonsgegevens en de ernst van de mogelijke gevolgen.	Mogelijk dient de inbreuk niet te worden gemeld/meegedeeld als er geen gevoelige gegevens zijn onthuld en als er slechts een klein aantal e-mailadressen is onthuld.