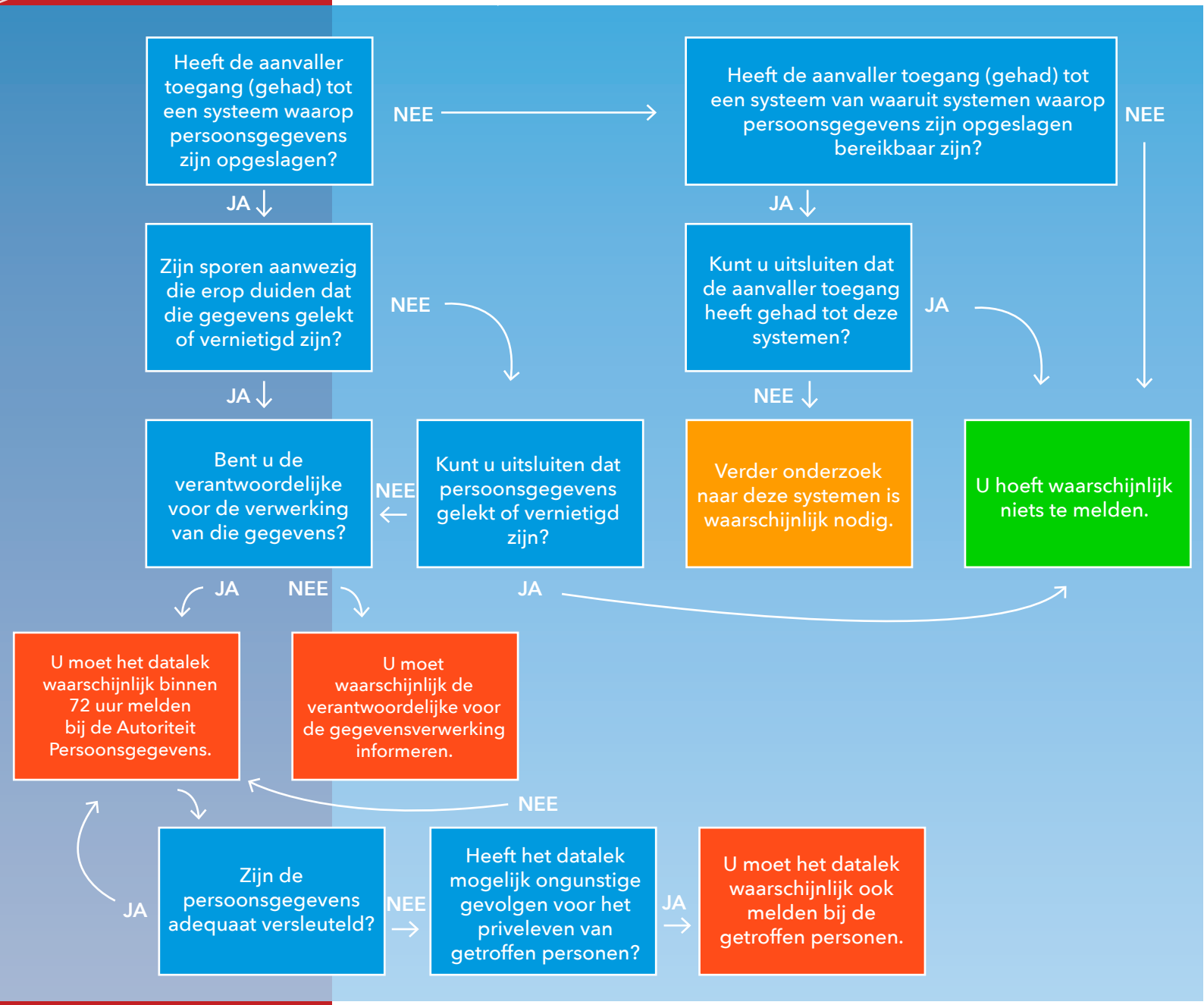

Meldplicht datalekken Stappenplan

Met bovenstaande infographic heeft u alle relevante informatie bij de hand. Zorg dat deze informatie bekend is bij het hoger- en middenmanagement. Laat u ook altijd adviseren door een gespecialiseerd jurist of advocaat voordat u besluit de Autoriteit Persoonsgegevens op de hoogte te stellen.

Hulp nodig?
Bel KICK-ICT voor assistentie.

070 – 799 0 799

Meldplicht datalek

Sinds 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) uitgebreid met de meldplicht datalekken. Dit houdt in dat bedrijven en overheden, in geval van een ernstig datalek waarbij persoonsgegevens mogelijk ongewenst openbaar worden gemaakt, meteen melding moeten doen bij de Autoriteit Persoonsgegevens.

Wat is een datalek?

Er is sprake van een datalek als derden, die geen toegang zouden mogen hebben tot bepaalde persoonsgegevens, toch die informatie in handen krijgen. In de meeste gevallen zal dit gepaard gaan met een beveiligingsincident.
Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Er is echter alleen sprake van een meldplicht, als er bij het datalek persoonsgegevens verloren zijn gegaan.

Wat zijn gevoelige persoonsgegevens?

- gegevens over godsdienst, levensovertuiging, ras, politieke overtuiging, gezondheid, seksleven, lidmaatschap of strafrechtelijke informatie;
- financiële gegevens als schulden of salaris- en betalingsgegevens.
  gegevens over verslavingen, schoolprestaties of werk- of relatieproblemen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude. Denk hierbij aan identiteitsbewijzen, paspoorten en Burgerservicenummers.

Moet u ieder datalek melden?

Nee zie hiervoor het stappenplan. Als stelregel voor melding kunt u aanhouden:
Als het gaat het om persoonsgegevens van gevoelige aard, of er is om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens.

Wanneer melden aan de betrokkene?

Als niet alle gelekte gegevens (goed) versleuteld waren, of het datalek heeft om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene.

25 mei 2018

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De belangrijkste wijzigingen:

- nog meer verplichtingen voor verwerkers van persoonsgegevens;
- nog meer rechten voor betrokkenen;
- nog meer formaliteiten;
- nog hogere boetes.

Ons advies aan u:

- IT Manager: Kies voor encryptie (versleuteling) van bestanden met persoonsgegevens, naast netwerk- en endpointsecurity;
- Medewerkers: Weet waar de gevaren schuilen, hoe met deze gevaren om te gaan en welke stappen je moet ondernemen als het misgaat;
- Bestuurder: Ontwikkel een gedegen securitybeleid en zorg voor Security Awareness binnen de organisatie.

Voor meer informatie kijkt u op de website van de Autoriteit Persoonsgegevens.

KICK-ICT
T | 070 – 799 0 799
E | info@kick-ict.nl

www.kick-ict.nl