

Checklist classificatie van gegevens

Op de volgende pagina's vind je een checklist waarmee je gegevens in je bedrijf kunt classificeren (digitaal, maar ook op papier). Door een classificatie van gegevens te maken kun je als bedrijf makkelijker vaststellen wat het beveiligingsniveau is van de gegevens die je bezit. Het is dus een soort checklist om passende beveiligingsmaatregelen te kunnen nemen. Immers, niet iedere stukje data hoeft even zwaar beveiligd te zijn maar sommige wil je juist extra goed beschermen.

Het classificeren van gegevens is een onderdeel van het in kaart brengen van passende beveiligingsmaatregelen. Uiteindelijk is het beter om de bedrijfsprocessen te classificeren. Voor het inrichten van de beveiliging kun je gebruik maken van de Code voor Informatiebeveiliging, ISO 27002 die wordt uitgegeven door de NEN.

Voor het in kaart brengen van de processen waarbij (potentieel) gevoelige gegevens worden verwerkt, kun je ook nog eens kijken naar de tool op www.beschermjebedrijf.nl voor de afhankelijkheid van ICT.

Invulinstructie

Bij de categorieën op de volgende pagina dien je steeds voor jezelf de volgende vragen te beantwoorden en het bijbehorende niveau van kwetsbaarheid aan te vinken:

Integriteit

Hoe erg is het als de betreffende gegevens ongemerkt worden veranderd tijdens verzending of wanneer gegevens zijn opgeslagen? Hoe erg is het als de identiteit van de afzender van de betreffende gegevens niet kan worden geverifieerd?

(Laag: geen enkel gevolg voor de bedrijfsvoering, Baseline: storend, maar oplosbaar probleem, Hoog: forse schade (in tijd/geld/imago), Zeer hoog: kan leiden tot faillissement, rechtszaak e.d.).

Vertrouwelijkheid

Hoe erg is het als de betreffende gegevens bij de verkeerde ontvanger terechtkomen? Hoe erg is het als deze gegevens publiekelijk worden verspreid?

(Laag: geen enkel gevolg voor de bedrijfsvoering, Baseline: storend, maar oplosbaar probleem, Hoog: forse schade (in tijd/geld/imago), Zeer hoog: kan leiden tot faillissement, rechtszaak e.d.)

Beschikbaarheid

Hoe erg is het als de betreffende gegevens niet op korte termijn beschikbaar zijn of kunnen worden gemaakt?

(Laag: het is geen probleem als de gegevens nooit meer boven water kunnen worden gehaald, Baseline: de gegevens mogen een paar dagen niet beschikbaar zijn voordat forse schade (in tijd/geld/imago) optreedt, Hoog: de gegevens mogen enige uren niet beschikbaar zijn voordat forse schade optreedt, Zeer hoog: de gegevens moeten altijd vrijwel onmiddellijk beschikbaar zijn, anders treedt schade op)

Deze checklist is overgenomen van het programma Kwint (2005), Veilig zakelijk internetten.

Persoonsgegevens

		laag/nvt	baseline	hoog	zeer hoog
NAW-gegevens (naam, adres, woonplaats)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Extra NAW-gegevens (privé mailadres, telefoonnummer, etc.)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Persoonlijke gegevens (burgerservicenummer (BSN), burgerlijke staat, godsdienst, ras)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Fiscale gegevens (belastingaangifte, bankafschriften)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
BKR-gegevens (Bureau Krediet Registratie)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Justitiële gegevens (strafblad, boetes, etc)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Gegevens m.b.t. sociale activiteiten (lid verenigingen)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Medische gegevens	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Gegevens m.b.t. communicatiegedrag (bel- en surfgedrag)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Beeldmateriaal van personen	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
(branchespecifiek, zelf in te vullen)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				

Bedrijfsgegevens		laag/nvt	baseline	hoog	zeer hoog
Contactgegevens klanten (naam, adres, plaats)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
NAW-gegevens contactpersonen en klanten of extra NAW-gegevens (privé mailadres, telefoonnummer, etc.) – zie persoonsgegevens	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Bijzondere persoonlijke gegevens, zoals bedoeld in de Wet Bescherming Persoonsgegevens (godsdienst, ras, gezondheid, seksuele leven) – zie persoonsgegevens	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Websitegegevens	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Gegevens Kamer van Koophandel	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Intellectueel eigendom (broncodes, recepten, nog niet uitgebrachte muziek, etc.)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Klantgegevens (ordergeschiedenis, bank/creditcard gegevens, accountgegevens, etc.)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Overige concurrentiegevoelige gegevens (offertes, e.d.)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Financiële gegevens (niet openbaar)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Personeelsgegevens (NAW-gegevens, personeelsdossiers, BSN)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Koersgevoelige gegevens (niet openbaar en niet-financieel)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
Juridische gegevens (elektronische koopovereenkomst, contracten, etc.)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				
(branchespecifiek, zelf in te vullen)	<i>integriteit</i>				
	<i>vertrouwelijkheid</i>				
	<i>beschikbaarheid</i>				