Toelichting Privacyrisicomatrix (1/2)

Waarom deze privacyrisicomatrix?

Voor veel managementsystemen (o.a. ISO 9001, ISO 14001 en ISO 27001) is het een vereiste om privacyrisico's en -bedreigingen in kaart te brengen. Dit kan lastig zijn voor een organisatie die hier nog geen ervaring mee heeft . Een hulpmiddel is de veelgebruikte zgn. MAPGOOD-methode. Deze beschrijft de verschillende invalshoeken om naar privacyrisico's en -bedreigingen te kijken. MAPGOOD staat voor:

- **M**ens: de mensen die nodig zijn om het informatiesysteem te beheren en te gebruiken
- **A**pparatuur: de apparatuur die nodig is om het informatiesysteem te laten functioneren
- **P**rogrammatuur: de programmatuur waaruit het informatiesysteem bestaat
- **G**egevens: de gegevens die door het systeem worden verwerkt
- **O**rganisatie: de organisatie die nodig is om het informatiesysteem te laten functioneren
- **O**mgeving: de omgeving waarbinnen het informatiesysteem functioneert
- **D**iensten: de externe diensten die nodig zijn om het systeem te laten functioneren

Toelichting Privacyrisicomatrix (2/2)

Voor wie is deze privacyrisicomatrix bedoeld?

Deze privacyrisicomatrix is bedoeld voor privacy-coördinatoren of andere personen die verantwoordelijk zijn voor het beheersen van (privacy)risico's binnen de organisatie. Het is verstandig om bij het opstellen van de privacyrisicomatrix een team van meerdere personen vanuit verschillende disciplines binnen de organisatie samen te stellen. De Functionaris Gegevensbescherming (tweede lijn) kan hierbij adviseren. Daarnaast kan de FG deze privacyrisicomatrix onderdeel maken van het toezichtskader.

Hoe moet je deze privacyrisicomatrix gebruiken?

Bepaal eerst welk proces van verwerking van persoonsgegevens je uit je organisatie wilt analyseren. Maak daarna een chronologische beschrijving van de verschillende verwerkingsfases die de persoonsgegevens doorlopen. Verwerk deze vervolgens in de kolommen van de privacyrisicomatrix. In de volgende slides wordt per kolom uit de privacyrisicomatrix een toelichting gegeven hoe je (deels via drop down) de gegevens kunt invullen.

Algemeen: Hoe krijg ik de verwerking helder?

Welke persoonsgegevens ontvang je?

- Van welke (externe) partij krijg je de gegevens?
- Krijg je de gegevens rechtstreeks van betrokkene of via een andere/derde partij?
- Op welke manier ontvang je gegevens? (in een gesprek, digitale weg of fysieke weg)

Wat doe je met de persoonsgegevens?

- Hoe registreer je de binnenkomende gegevens? Waar sla je ze op? (applicatie, gegevensdrager of fysiek)
- Verrijk of koppel je gegevens? (o.b.v. een uniek nummer)
- Waarvoor gebruik je de gegevens? (klantregistratie, personeelsadministratie etc.)
- Is er ook sprake van ander gebruik dan waarvoor de gegevens zijn verkregen? (marketing, onderzoek, etc.)
- Hoe gebruik je de gegevens? (raadplegen, delen, actualiseren en verwijderen)
- Zijn de gegevens onderdeel van een rapportage en zo ja, op welke manier?

Welke persoonsgegevens verstrek je?

- Welke persoonsgegevens verstrek je aan een (externe) partij?
- Welke (externe) partij ontvangt de gegevens? (betrokkene of via een andere/derde partij)
- Op welke manier verstrek je de gegevens? (in een gesprek, digitale weg of fysieke weg)

Kolom B ‘Bedreiging’, toelichting op drop down

Mens

- Onkunde, slordigheid
- Niet werken volgens voorschriften
- Fraude, sabotage

Apparatuur

- Verouderd
- Functioneert onjuist
- Stroomuitval

Programmatuur

- Ontwerpfouten
- Programmeerfouten
- Geen actuele updates

Gegevens

- Ontoegankelijk
- Onterecht toegankelijk
- Gaan verloren
- Onbedoelde wijziging

Organisatie

- Onduidelijke taken, bevoegdheden
- Ontbrekende gedragscodes

Omgeving

- Ruimtes onvoldoende beveiligd
- Natuurgeweld

Diensten

- Geen goede leveranciersafspraken
- Leverancier gaat failliet

LUMEN GROUP privacy & data

Kolom C ‘Type’, toelichting op drop down

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Controle over de data
- Rechten van betrokkenen
- Transparantie
- Doelbinding en verder verwerking
- Rechtmatigheid verwerking
- Dataminimalisatie
- Opslagbeperking
- Locatie van de verwerking
- (Her)identificatie

LUMEN GROUP privacy & data

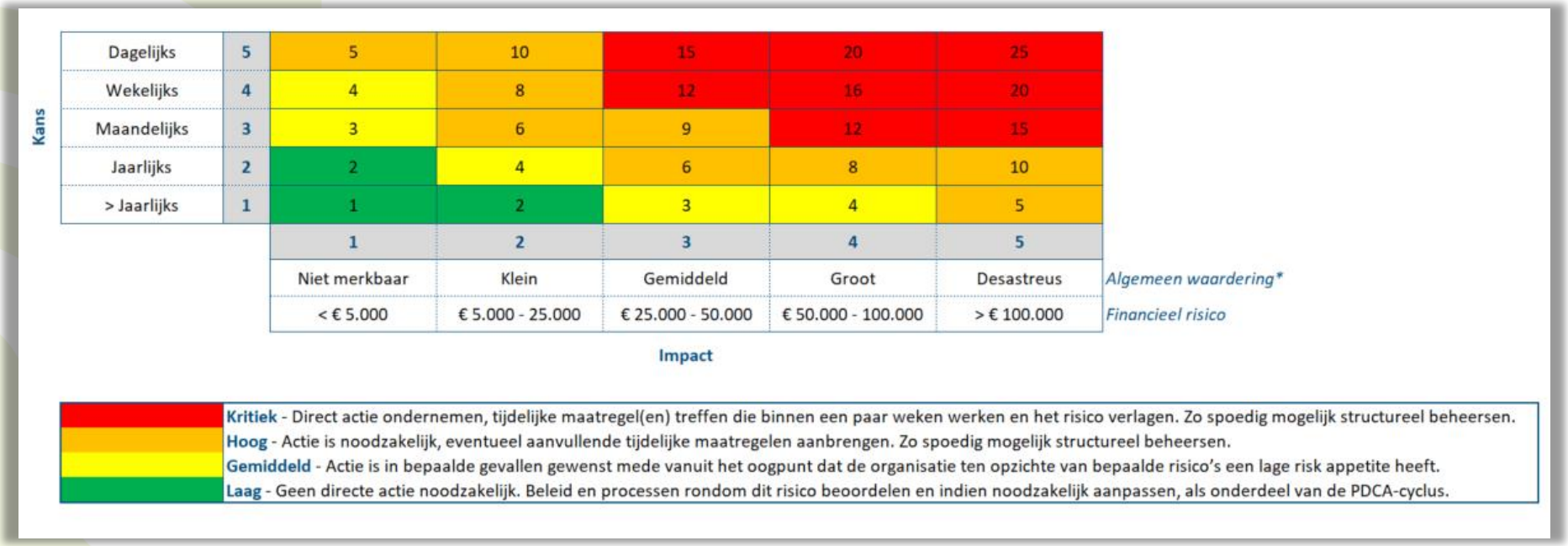
Kolom D ‘Risico’

- Neem de chronologische beschrijving van de verschillende stappen die de persoonsgegevens in het proces doorlopen als uitgangspunt
- Bepaal van elke stap in het proces het (potentiële) risico
- Omschrijf dit risico zo gedetailleerd mogelijk
- Gebruik voor elk risico een aparte regel

Kolom E ‘van toepassing op’

- Geef aan of het om je eigen organisatie / afdeling / leverancier gaat

Kolom F & G ‘Inschatting kans x impact’



Kans						
Dagelijks	5	5	10	15	20	25
Wekelijks	4	4	8	12	16	20
Maandelijks	3	3	6	9	12	15
Jaarlijks	2	2	4	6	8	10
> Jaarlijks	1	1	2	3	4	5
		1	2	3	4	5
		Niet merkbaar	Klein	Gemiddeld	Groot	Desastreus
		< € 5.000	€ 5.000 - 25.000	€ 25.000 - 50.000	€ 50.000 - 100.000	> € 100.000

*Algemeen waardering**

Financieel risico

Impact

	Kritiek - Direct actie ondernemen, tijdelijke maatregel(en) treffen die binnen een paar weken werken en het risico verlagen. Zo spoedig mogelijk structureel beheersen.
	Hoog - Actie is noodzakelijk, eventueel aanvullende tijdelijke maatregelen aanbrengen. Zo spoedig mogelijk structureel beheersen.
	Gemiddeld - Actie is in bepaalde gevallen gewenst mede vanuit het oogpunt dat de organisatie ten opzichte van bepaalde risico’s een lage risk appetite heeft.
	Laag - Geen directe actie noodzakelijk. Beleid en processen rondom dit risico beoordelen en indien noodzakelijk aanpassen, als onderdeel van de PDCA-cyclus.

Dit is een voorbeeld risicomatrix. De inschatting van kans en impact is altijd subjectief. Maak hier afspraken over.

LUMEN GROUP privacy & data

Kolom I (e.v.) ‘Beheersmaatregelen’

Preventie

- Voorkomen dat iets gebeurt of het verkleinen van de kans daarop

Detectie

- Tijdig signaleren van de (potentiële) schade wanneer een bedreiging optreedt

Mitigatie

- Beperken van de schade wanneer een bedreiging optreedt

Correctie

- Maatregelen om het effect (deels) terug te draaien

Acceptatie

- Geen (additionele) maatregelen, weloverwogen accepteren van kans en gevolgen

Overdragen

- Financieel (verzekeren) of operationeel (outsourcen)

- Omschrijf de te nemen/genomen beheersmaatregelen zo specifiek mogelijk: gebruik bovenstaande algemene maatregelen als leidraad
- Bepaal op basis van deze beheersmaatregelen in de kolommen J & K ‘inschatting’ opnieuw de kans x impact (zie voor weging slide 4)
- Bepaal vervolgens in kolom M of het restrisico ja/nee acceptabel is
- Omschrijf in kolom N eventuele aanvullende beheersmaatregelen
- Leg in kolom O vast of de evt. aanvullende maatregelen akkoord zijn (door bijv. de proceseigenaar).

LUMEN GROUP privacy & data