Status: Vastgesteld MT-LISA
Datum goedgekeurd: 14-11-2023
Auteur: Annika van der Putten

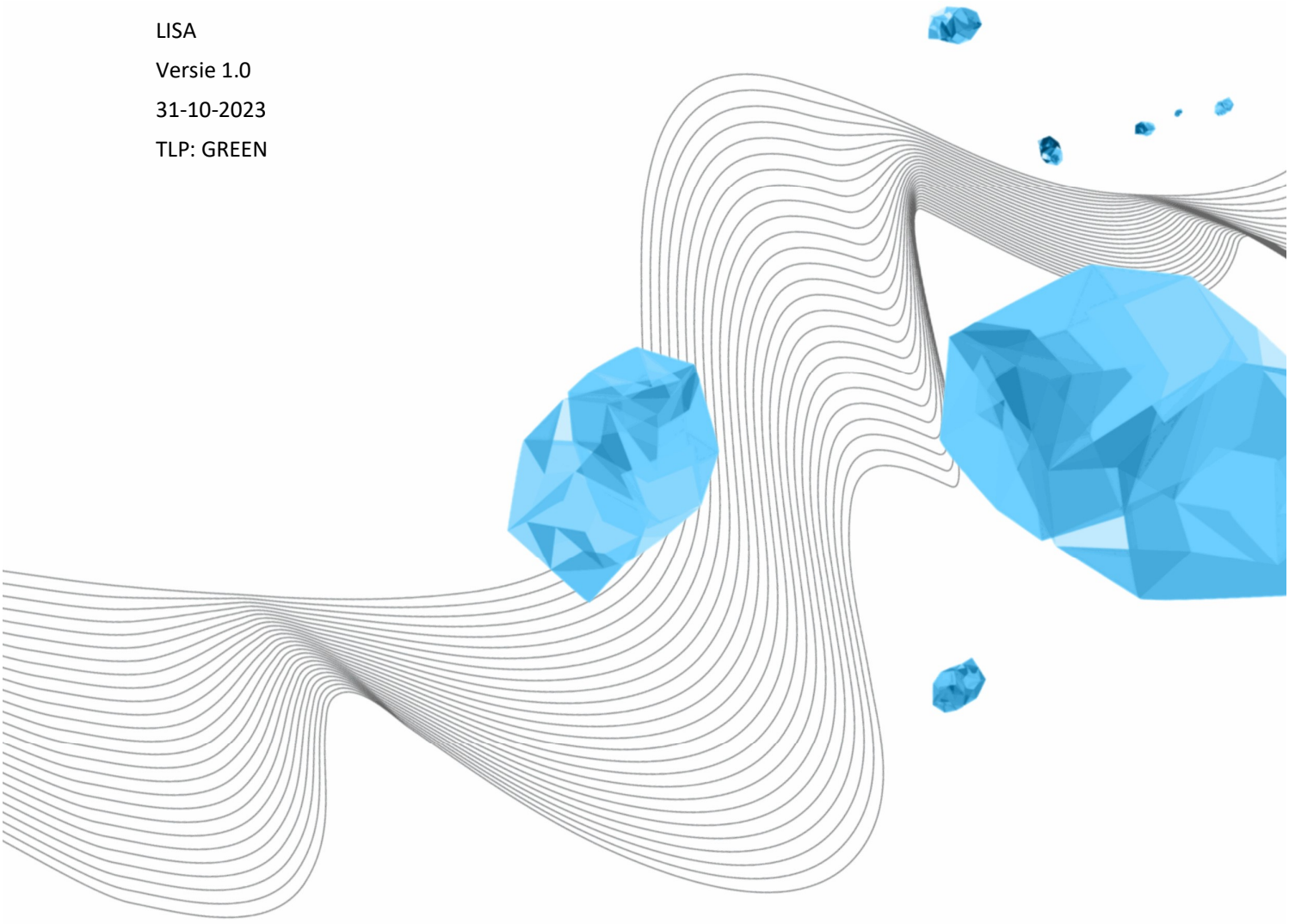
METHODIEK DPIA UNIVERSITEIT TWENTE

LISA

Versie 1.0

31-10-2023

TLP: GREEN



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Methodiek DPIA Universiteit Twente

KENMERK
LISA-403

VERSIE (STATUS)
1.0

DATUM
31-10-2023

AUTEUR(S)
Annika van der Putten

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	31-10-2023	Annika van der Putten	

DISTRIBUTIELIJST

VERSIE	DATUM	GEDISTRIBUEERD AAN	OPMERKING

INHOUDSOPGAVE

INLEIDING

Dit document beschrijft de methodiek voor het uitvoeren van Data Protection Impact Assessments (DPIA's) voor de Universiteit Twente, waarbij rekening wordt gehouden met onderwijs, onderzoek en bedrijfsvoering.

De AVG eist (artikel 35) dat bij bepaalde soorten van verwerking van persoonsgegevens voorafgaand een risico-beoordeling moet worden uitgevoerd. Deze risico-beoordeling wordt een Data Protection Impact Assessment genoemd. Dat geldt bijvoorbeeld voor verwerkingen waarbij nieuwe technologieën worden gebruikt of die op een andere manier een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

De methodiek in dit document moet worden geïntegreerd in de procedures van de Universiteit Twente om ervoor te zorgen dat DPIA's systematisch worden uitgevoerd voor alle relevante activiteiten op het gebied van onderwijs, onderzoek en bedrijfsvoering.

Het template voor een pre-DPIA op de cybersafety website kan dienen als een handig startpunt voor het verzamelen van informatie bij de start van elk project.

STAP 1: IDENTIFICATIE EN ORGANISATIE

1.1 PROJECT IDENTIFICATIE

Bij de start van elk project, onderwijsinitiatief, onderzoek of bedrijfsactiviteit waarbij persoonsgegevens worden verwerkt, moet een registratie van de voorgenomen verwerking plaatsvinden. Onderzoekers dienen dit te doen via het Datamanagementplan, terwijl bedrijfsvoering dit in overleg met de Privacy Contact Persoon (PCP) van desbetreffende faculteit of dienst, de Functionaris Gegevensbescherming (FG) of Privacy Officer (PO) vastlegt.

De verantwoordelijkheid voor het uitvoeren van een (pre-)DPIA ligt bij de afdeling/medewerker zelf, maar de uitvoering zal gebeuren met advies en ondersteuning van de PO en/of FG.

1.2 VASTSTELLEN VAN DE NOODZAAK

Vervolgens zal moeten worden beoordeeld of de verwerking van persoonsgegevens waarschijnlijk een hoog risico met zich meebrengt voor de rechten en vrijheden van betrokkenen. Gebruik hiervoor het template voor een pre-DPIA op de cybersafety website als leidraad.

Indien er sprake is van een (mogelijk) hoog risico verwerking, dan wordt een DPIA uitgevoerd conform het standaard template *Data protection impact assessment* van [datum]. Hiervoor wordt een DPIA-team samengesteld (zie hierna).

1.3 DPIA-TEAM SAMENSTELLEN

Stel samen met de PCP van desbetreffende dienst/faculteit een multidisciplinair DPIA-team samen, bestaande uit vertegenwoordigers van onderwijs, onderzoek, bedrijfsvoering, de FG/PO en eventueel andere relevante experts.

STAP 2: GEGEVENSVERZAMELING EN BEOORDELING

2.1 VERZAMEL GEGEVENS

Verzamel alle relevante informatie over de gegevensverwerking, inclusief:

- de aard en omvang van de verwerkte gegevens,
- de categorieen van de persoonlijke gegevens,
- de doeleinden van de verwerking,
- de betrokkenen en ontvangers van de gegevens,
- de opslaglocatie en de bewaartermijn van de verwerkte gegevens,
- welke technieken en methodes gehanteerd worden om de gegevens te verwerken,
- hoe rechten van betrokkenen worden geimplementeerd.

2.2 RISICOBEOORDELING

Voer een gedetailleerde risicobeoordeling uit. Beoordeel de mogelijke impact van de verwerking op de rechten en vrijheden van betrokkenen, inclusief de kans op inbreuken op de gegevensbescherming.

STAP 3: MAATREGELEN EN AANBEVELINGEN

3.1 IDENTIFICEER MAATREGELEN

Identificeer passende technische en organisatorische maatregelen om de risico's te minimaliseren. Overweeg pseudonimisatie, anonimisatie, versleuteling en andere privacyversterkende maatregelen.

3.2 IMPACTVERMINDERING

Beoordeel de effectiviteit van de voorgestelde maatregelen in het verminderen van de risico's. Bepaal of er aanvullende maatregelen nodig zijn.

3.3 RAPPORTAGE EN DOCUMENTATIE

Documenteer alle bevindingen, maatregelen en aanbevelingen in een DPIA-rapport. Dit rapport moet worden gedeeld met alle relevante belanghebbenden, waaronder het DPIA-team, de FG/Privacy Officer en het management.

Nadat de DPIA opgesteld zal deze ter advisering worden aangeboden aan de FG (artikel 35 lid 2).

Het advies van de FG wordt opgenomen in het DPIA-rapport. Daarbij wordt aangegeven of/en op welke manier het advies is opgevolgd.

STAP 4: AUTORISATIE EN IMPLEMENTATIE

4.1 AUTORISATIE

Indien de adviezen van de FG zijn opgevolgd en verwerkt in het DPIA-rapport, dan kan worden gestart met de verwerking van de gegevens.

Mocht er worden afgeweken van het advies van de FG, zal het DPIA-rapport moeten worden beoordeeld en goedgekeurd door het management van de betrokken afdeling of project. De uitkomst moet worden meegenomen in het DPIA-rapport. Na goedkeuring kan worden gestart met het verwerken van de gegevens.

Het DPIA-rapport wordt oa opgeslagen op de Teamspagina van de FG.

4.2 IMPLEMENTATIE

Implementeer de goedgekeurde maatregelen en zorg ervoor dat deze worden opgenomen in het project of de bedrijfsvoering.

STAP 5: MONITORING EN BIJSTELLING

5.1 MONITORING

Houd de gegevensverwerking en de effectiviteit van de genomen maatregelen regelmatig in de gaten. Een DPIA moet minimaal om de 3 jaar opnieuw worden beoordeeld.

5.2 BIJSTELLING

Indien nodig, stel de DPIA bij op basis van nieuwe risico's of wijzigingen in de verwerking.