Status: Approved MT-LISA
Date approved: 14-11-2023
Author: Annika van der Putten

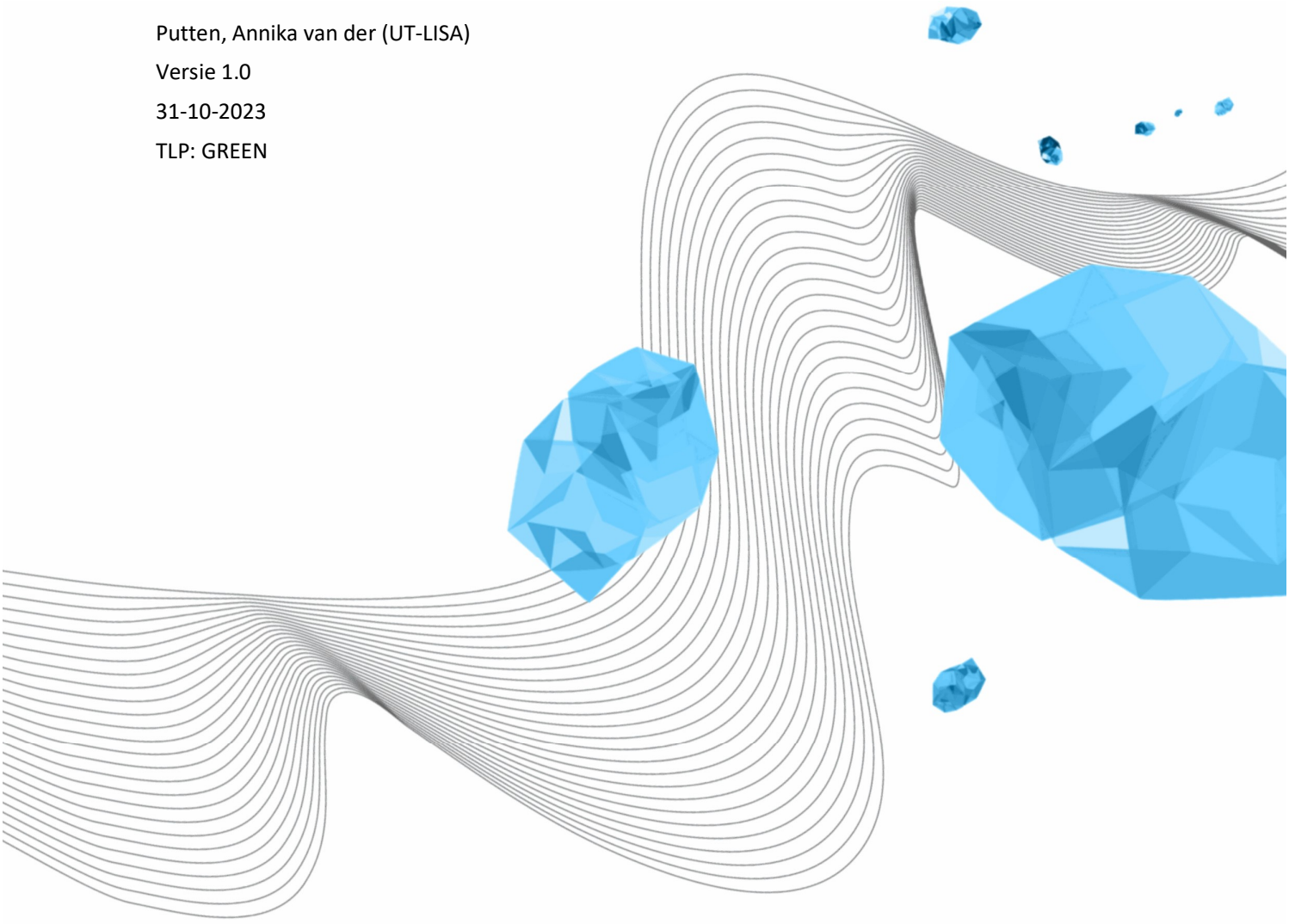
METHODOLOGY DPIA UNIVERSITY OF TWENTE

Putten, Annika van der (UT-LISA)

Versie 1.0

31-10-2023

TLP: GREEN



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Methodology DPIA University of Twente

KENMERK
LISA-403

VERSIE (STATUS)
1.0

DATUM
31-10-2023

AUTEUR(S)
Annika van der Putten

DOCUMENT HISTORY

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

DISTRIBUTIELIJST

VERSIE	DATUM	GEDISTRIBUEERD AAN	OPMERKING

INHOUDSOPGAVE

INTRODUCTION

This document describes the methodology for conducting Data Protection Impact Assessments (DPIAs) for the University of Twente, taking into account teaching, research and business operations.

The AVG requires (Article 35) that a risk assessment must be carried out prior to certain types of processing of personal data. This risk assessment is called a Data Protection Impact Assessment. This applies, for example, to processing operations that use new technologies or otherwise pose a high risk to the rights and freedoms of data subjects.

The methodology in this document should be integrated into the University of Twente's procedures to ensure that DPIAs are carried out systematically for all relevant teaching, research and business operations activities.

The template for a pre-DPIA on the cybersafety website can serve as a convenient starting point for gathering information at the start of each project.

STAP 1: IDENTIFICATION AND PLANNING

1.1 Project Identification

At the start of any project, educational initiative, research or business activity that involves processing personal data, a record of the intended processing must be made. Researchers should do this through the Data Management Plan, while business management should record this in consultation with the Privacy Contact Person (PCP) of relevant faculty or department, the Data Protection Officer (FG) or Privacy Officer (PO).

The responsibility for conducting a (pre-)DPIA lies with the department/employee itself, but implementation will be done with advice and support from the PO and/or FG.

1.2 ESTABLISHING THE NEED OF A DPIA

It will then be necessary to assess whether the processing of personal data is likely to pose a high risk to the rights and freedoms of data subjects. For this, use the template for a pre-DPIA on the cybersafety website as a guide.

If there is (potentially) high risk processing, a DPIA is carried out in accordance with the standard template Data protection impact assessment from [date]. A DPIA team is put together for this purpose (see below).

1.3 ASSEMBLE DPIA-TEAM

Together with the PCP of relevant department/faculty, assemble a multidisciplinary DPIA team consisting of representatives from education, research, operations, the FG/PO and possibly other relevant experts.

STAP 2: DATA COLLECTION AND ASSESSMENT

2.1 COLLECTING DATA

Collect all relevant information on the data processing, including:

- the nature and scope of the data processed,
- the categories of personal data,
- the purposes of the processing,
- the data subjects and recipients of the data
- the storage location and the retention period of the data processed
- what techniques and methods are used to process the data,
- how data subjects' rights are implemented.

2.2 RISK ASSESSMENT

Conduct a detailed risk assessment. Assess the potential impact of the processing on the rights and freedoms of data subjects, including the likelihood of data protection breaches.

STAP 3: MEASURES AND RECOMMENDATIONS

3.1 IDENTIFY MEASURES

Identify appropriate technical and organisational measures to minimise risks. Consider pseudonymisation, anonymisation, encryption and other privacy-enhancing measures.

3.2 IMPACT REDUCTION

Assess the effectiveness of the proposed measures in reducing risks. Determine whether additional measures are needed.

3.3 REPORTING AND DOCUMENTATION

Document all findings, actions and recommendations in a DPIA report. This report should be shared with all relevant stakeholders, including the DPIA team, the FG/Privacy Officer and management.

After the DPIA has been prepared, it will be submitted to the FG for advice (Article 35(2)).

The FG's advice will be included in the DPIA report. It will be indicated whether/and in what way the advice was followed.

STAP 4: AUTORISATION AND IMPLEMENTATION

4.1 AUTORISATION

Document all findings, actions and recommendations in a DPIA report. This report should be shared with all relevant stakeholders, including the DPIA team, the FG/Privacy Officer and management.

After the DPIA has been prepared, it will be submitted to the FG for advice (Article 35(2)).

The FG's advice will be included in the DPIA report. It will be indicated whether/and in what way the advice was followed.

4.2 IMPLEMENTATION

Implement the approved measures and ensure they are incorporated into the project or operations.

STAP 5: MONITORING AND ADJUSTMENT

5.1 MONITORING

Regularly monitor data processing and the effectiveness of the measures taken. A DPIA should be reviewed at least every 3 years.

5.2 ADJUSTMENT

If necessary, update the DPIA based on new risks or changes in processing.