STRATEGY DATA PROTECTION TILBURG UNIVERSITY

From unconscious risk taking to controlled risk management

1-12-2017

Preface

Data Protection is an important prerequisites for the services that we provide as a university. This means that also information security is of big importance.
In our strategic plan 2018-2021 called Connecting to Advance Society we have addressed our vision in a rapidly changing environment. Our core values are defined as a passion for truth, reliability, connectivity, empathy, inclusiveness, transparency, entrepreneurial thinking and responsibility. In our strategy we also emphasize our Corporate Social Responsibility.

In this context we can also relate to Data Protection. As we need to be a reliable, transparent partner we also need to ensure that we handle the data we have of our students, staff members and other individuals with the utmost care. Service delivery instills trust: get it right the first time, deliver on time and do it for an excellent price in order to be trustworthy and satisfy our customers in the various processes (e.g. students, employees, partners).

It is therefore very important that we comply with the law and legislation with regard to Data Protection with regard to personal data which is formalized in the General Data Protection Regulation (GDPR) also mentioned as Algemene Verordening Gegevensbescherming (AVG) which will be applicable from May 25, 2018. If we consider that based on our risk assessment we need additional measures (on top of the requirements in the law), we will implement them.

In this strategic document we formalize our strategy with regard to Data Protection. In order to realize this strategy it is important that we define our internal policies. There is a strong link with the Information Security Policy for the technical and organization security to ensure privacy. Furthermore we have defined a Tilburg University Data Protection Policy.

Executive Board

12 december 2017

1. Introduction

1.1. Content

In this document we formalize the strategy by Tilburg University with regard to Data Protection:

- What is our ambition?
- Are we prepared to take risk? And which?
- How do we measure the various interest? For example Data Protection in relation to innovation and research)
- What are the responsibilities with regard to Data Protection?
- How do we ensure the knowledge and skills?
- What are the mandatory elements to ensure compliance?
- What are the means?

1.2. Version Management

Version	Date	Content	Author	Validation by	Approval
1.0	12-12-2017	• First version	Jolanda Peters	Kernteam privacy	Executive Board

2. Definitions

In this chapter the definitions that are used in this strategy are defined.

	Definition
Algemene Verordening Gegevens-verwerking (AVG)	General Data Protection Regulation.
Consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (article 4.11 GDPR)
Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Data Protection	Data Protection refers to the processing in line with the GDPR and is referred to the law which is commonly defined to protect personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system
Data Protection Agreement	Agreement that is formalized between the controller and processor of data that formalizes the responsibilities of both parties and which is mandatory according to the GDPR.
Data Protection Authority	Autoriteit Persoonsgegevens (AP) is the independent public supervising authority regarding Data Protection in the Netherlands
Data Processing Impact Assessment	An assessment of the impact of the envisaged processing operations on the protection of personal data
General Data Protection Regulation (GDPR)	Law issued by the European Union with regard to data protection. The Dutch name of the law is Algemene Verordening Gegevensverwerking.
Personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (article 4.1 GDPR)
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. (article 4.12 GDPR)
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Record of Processing activities	Registration (database) that contains all the processing regarding personal data within Tilburg University as required by the GDPR. In Dutch: verwerkingsregister.
Special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (article 9 GDPR)
Uitvoeringswet AVG	National law and legislation that defines rules for the execution of the GDPR.

3. Law and legislation

The following law and legislation is applicable and taken into account into this strategy:

English	Dutch	version
General Data Protection Regulation (GDPR)	Algemene Verordening Gegevensbescherming (inclusief uitvoeringswet)	27-4-2016
	Uitvoeringswet AVG	In consultation
Telecommunication law	Telecommunicatiewet	19-10-1998

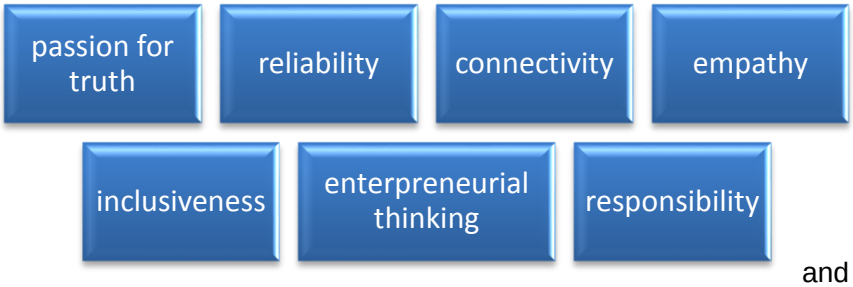
4. Strategic relevance Data Protection within Tilburg University

The world with regard to information management is rapidly changing. Developments like increasing digitalization, alternative storing locations (for example cloud, off location), increasing data transfer (exchange of data with other parties within the Netherlands, within the European Union or abroad), big data increase the risks related to information management. Furthermore the external threats increase for example caused by cybercrime. This development will continue in the coming period, and the related risks will also increase, having an effect on Data Protection.
The number of reported incidents with regard to data protection and privacy have increased substantially over the past few years. In 2016 the Dutch regulator: Autoriteit Persoonsgegevens (AP) has received 5.700 reported incidents[1] compared with 4.500 in 2015. This increase is due to the increase of the risks, but also due to the increase of the awareness of individuals with regard to their privacy. People are getting more aware about their privacy.

But as Barack Obama has stated:

> *'It is important to realize that you cannot have 100% security and then have 100% privacy and zero inconvenience. We are going to have to make some choices.'*

For Tilburg University information is a very important asset. In the Strategic Plan 2018-2021 called connecting to advance society we have defined our core values:

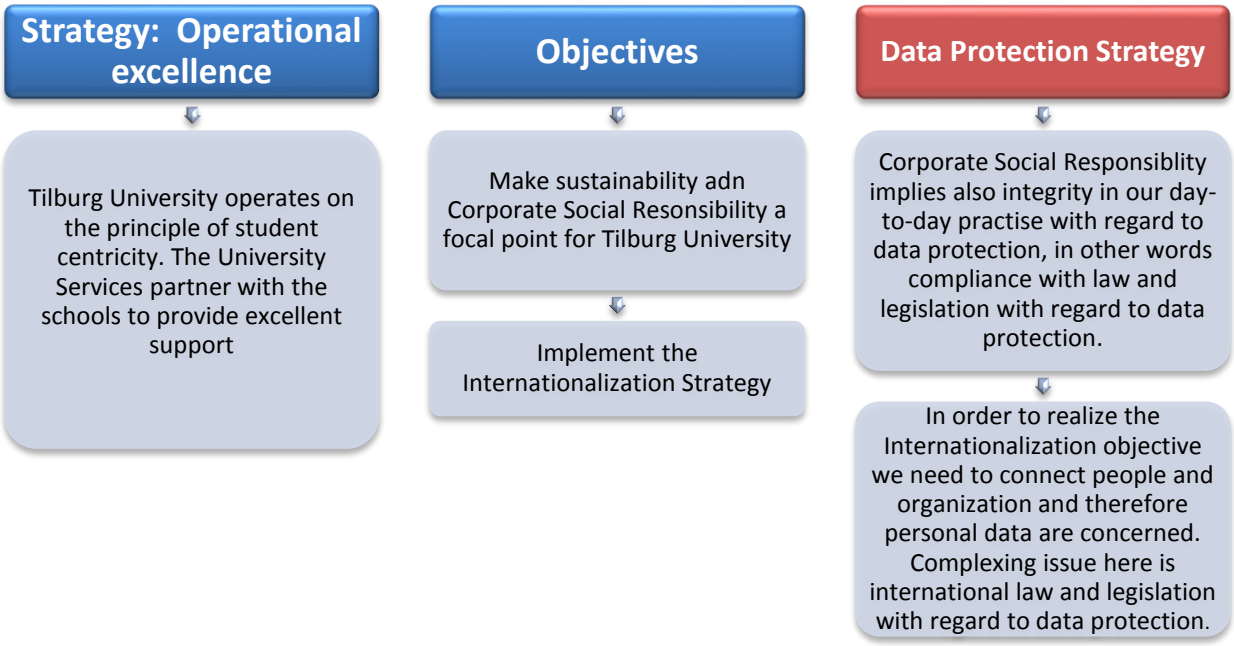


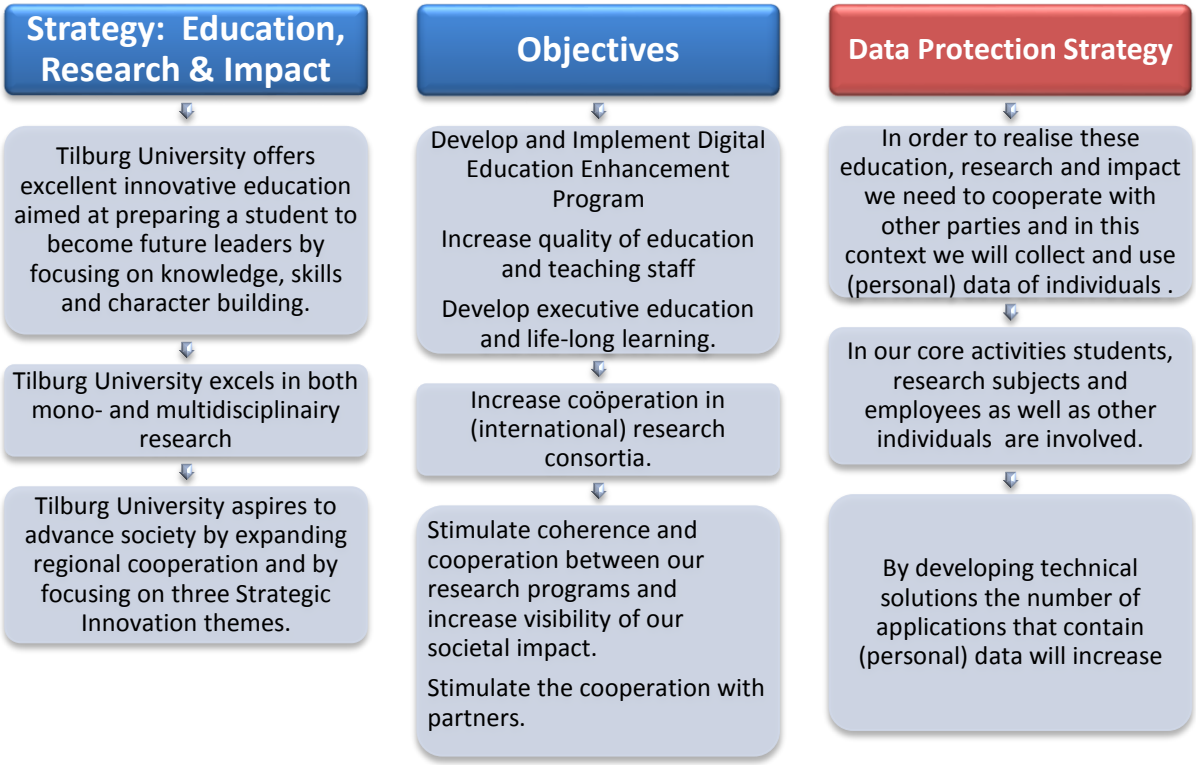
Privacy and data protection can be seen in relation to these corporate values especially:

[1] Source: jaarverslag autoriteit persoonsgegevens

- Connectivity: in order to be able to connect we need and use personal data.
- Reliability: in order to be reliable we need to ensure that we are transparent to our relations / stakeholders and keep our promises. This also encounters for personal data: we must be transparent in what and why we process them, and actively inform the customer. On request of the customer we must inform, remove or adjust the data.
- Responsibility: we take our responsibility as organization and ensure that we are compliant with all vigilant law and legislation with regard to personal data.

Furthermore the reputational risk regarding incidents with regard to Data Protection is very high. Especially as Tilburg University provides education and performs research on the areas GDPR, Law and Technology and Data science. Finally we have defined our strategic objectives:





Data Protection is applicable in all of Tilburg University's activities and is an important prerequisite in setting the standard for realizing our strategic goals. It is important that the policies with regard to Data Protection are clearly defined and that the security measures (technical and organizational) are adequate. We refer to 2 policies which are heavily related in order to secure this:

- Information security Policy (***informatiebeveiligingsbeleid)***
- Data Protection Policy (***Tilburg University Data Protection Policy***)

5. Trends, developments and risks

5.1. Technological trends

Due to technological developments, innovations, the linking of data e.g. by working from location, working in the cloud, open data, big data and exchange of information, the University has access to more and more data. Via mobile technology we have real-time access to information from all locations. This has many advantages (e.g. convenience) but there is also a risk: unauthorized access and the (excessive) processing of (personal) data.

The trends are mainly related to digital. The developments are continuing to be extremely fast. For example the 'smart' technology, smart meters, smart appliances, smart phones etc. Tilburg University is also involved in these developments.

5.1.1. Big data

Big data are becoming more and more important in every organization and can be used in order to predict, prevail or safe. Think about monitoring, investigations etc. For research purposes but also for supporting processes the use of big data will increase further which will have an impact on data protection and privacy (increase of risk).

5.1.2. Cloud Services

The storage of data is increasingly done at another location for example in the 'cloud'. The level of impact by Tilburg University in order to safeguard this information is decreasing, as the storage facility is not managed by Tilburg University. Therefore the risk of incidents with regard to data protection and privacy is increasing.

5.1.3. Internet of Things

It is no longer only people and organization that are connected digitally. More and more objects are becoming a 'computer' from cars, to copying machines to refrigerators. Camera's in public arears recognize faces and transport patterns.
All these appliances communicate with each other and their users and making it 'smart'. Your phone tells you where your car is parked, and how long the commute to home is (using big data), in other words 'the internet of things', which has an impact on privacy and data protection (increase of risks).

5.1.4. Wearables / GPS

Wearables e.g. smart watches, Fitbit are more and more common in the world. TiU uses wearables in various research projects in Tilburg School of Social and Behavioural Sciences. We expect that the usage by these means will increase in the near future, e.g. GPS-registration of students, measuring health of employees etc.

5.1.5. Virtual reality – Augmented reality

Virtual reality and augmented reality are currently only exploited in the gaming-industry. The boundary between reality and virtual reality is getting smaller. However the first steps are already made in training and education depending on the development of applications (apps).

5.2. External threats and dependencies

Due to the above trends and developments data protection and privacy is under pressure. On top of this there are (inter)national developments and dependencies that affect TiU and therefore are risks. They will be assessed as part of the risk mapping to identify whether controls are required. For more detail we refer to the *risk management & control standard and charter.*

On an annual basis the National Cyber Security Centrum (part of the Ministry of Justitie en Veiligheid) issues the Cybersecuritybeeld Nederland. This lists the threats and trends with regard to cybersecurity.

5.2.1. Cryptoware and Ransomware

Cryptoware[2] and ransomware[3] are the business models behind cybercrime. The income that criminals realize with cryptoware and ransomware are high. Data will be released after the payment of a ransom. The expectation is that the number of ransomware and cryptoware attacks will further increase, and related risks with regard to privacy and data protection therefore is increasing.

5.2.2. Phishing

Phishing (the phishing to login details) is playing a key role with regard to dedicated digital attacks. Phishing emails are more and more difficult to identify and are an easy and effective attack instrument. With a successful phishing attack the criminal will get access to internal networks and (personal) data.
Tilburg University can be used in a digital attack (use our information to get personal data of students, employees) and/or our networks can be attacked using phishing email.

5.2.3. Need for Availability is increasing

Important processes will stop if the IT-systems and/or alternatives are not available. The dependency of supporting IT systems is increasing, and there are less alternatives available. This increases the risk of non-availability. For the core processes of the university (education and research) the dependency on IT is growing (for example with digital testing). There are DdoS-attacks (Distributed denial of Service) that will affect the non-availability risk.

5.2.4. Law and legislation

The law and legislation with regard to privacy and data protection is rapidly developing and the requirements are increasing. This is a result of the response to (technical) developments and the focus of individuals with regard to their right of privacy.

[2] Blackmail method via malware which will encrypt data which will become not accessible.
[3] Blackmail method via malware which takes computers as ‘hostage’ and they will become inaccessible (and can be released via payment)

5.3. Internal threats and dependencies

5.3.1. Inadequate knowledge and (digi)-skills

In order to protect data and privacy knowledge and digital skills are essential. Well educated staff is key to prevent incidents with regard to data protection and privacy. People need to be aware of the risks and why certain measures are implemented. This requires a constant level of education and communication with regard to date protection and privacy.

5.3.2. Unconscious behavior

Unconscious behavior often causes carelessness and non-adequate access to data. The challenge is to ensure constant awareness with regard to privacy and data protection.

5.3.3. Quick, always and everywhere

Due to the increasing digitalization and flexibilisation information must be accessible always from every (mobile) location. This puts privacy and data protection at risk. In order to mitigate this risk this aspect (privacy by design) must be taken into account into projects.

5.3.4. Unauthorized access

The premises, buildings, networks, information systems must be protected against unauthorized access. It must be secured that the risks of damage, theft of data and malfunction must be minimized. Access to IT systems (and (personal) data must be granted solely to authorized users.

6. Ambition

Tilburg has the ambition to fully comply with the GDPR, as it considers data protection as key. However 100% security and compliance with regard to data protection is a utopia mainly due to human failure.

As indicated Tilburg University wants to be a reliable and responsible organization. Students and other stakeholders must be able to trust us that we process their data in a careful way. Due to the developments described in chapter 5, this will be more and more complex.

Due to the implementation of the GDPR that will come into effect on 25 may 2018 the financial and reputational consequences of non-compliance will be a serious risk for Tilburg University. The media attention regarding Data Protection is increasing and also the sanctions that are issued by the supervisory Authority are increasing and on top of this they are changing their supervisory strategy (more stringent).

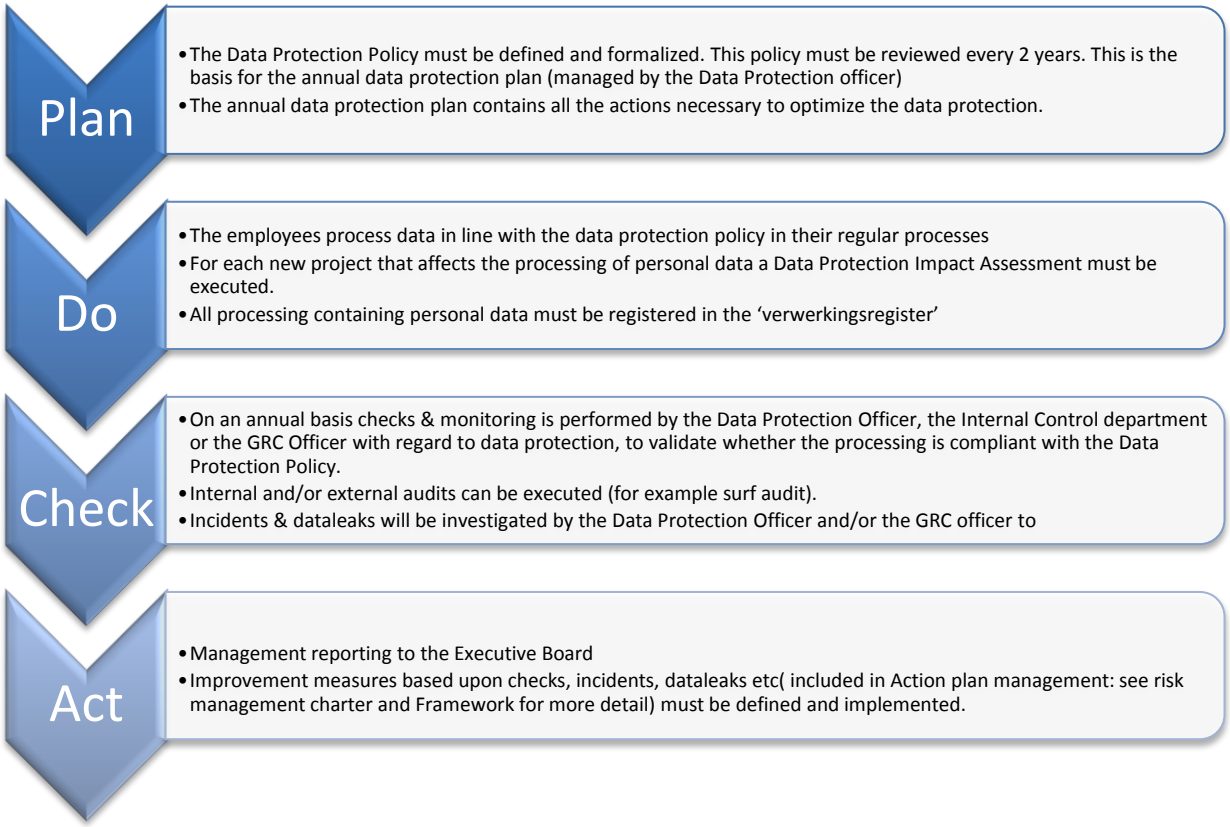
Information security and (Personal) Data Protection is always a cost-benefit analysis, as 100% security and compliance is a utopia. There will be weak links (often human) in every process and activity. Tilburg University strives to an optimal level of Data-Protection and Privacy in which we carefully balance the protection of privacy and the workability of the processes. The internal policies are formalized in the Data Protection Policy and the Information Security Policy.

6.1. Standard Framework (normenkader)

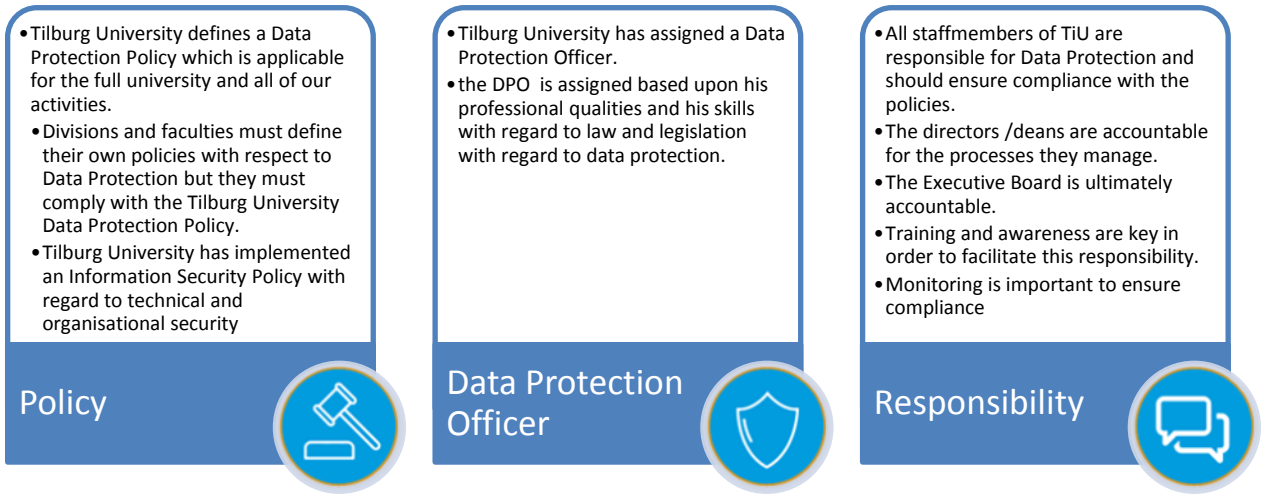
Currently there is no standard framework with regard to Data protection. It is under development on European Level and will then probably be available for the Netherlands via NEN-organization. The development will start end of 2017.
The ambition for Tilburg University is that we want to comply with this standard framework with regard to Data Protection.

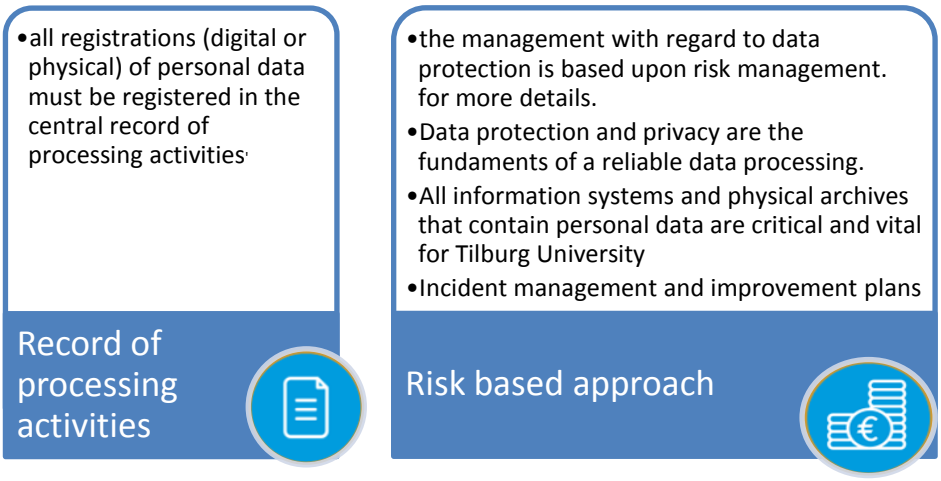
6.2. Continuous improvement

Because of the rapidly changing environment that affects data protection and privacy, we need to implement a continuous process to ensure compliance and mitigate the risks. We have therefore implemented an iterative process based upon Plan do Check Act



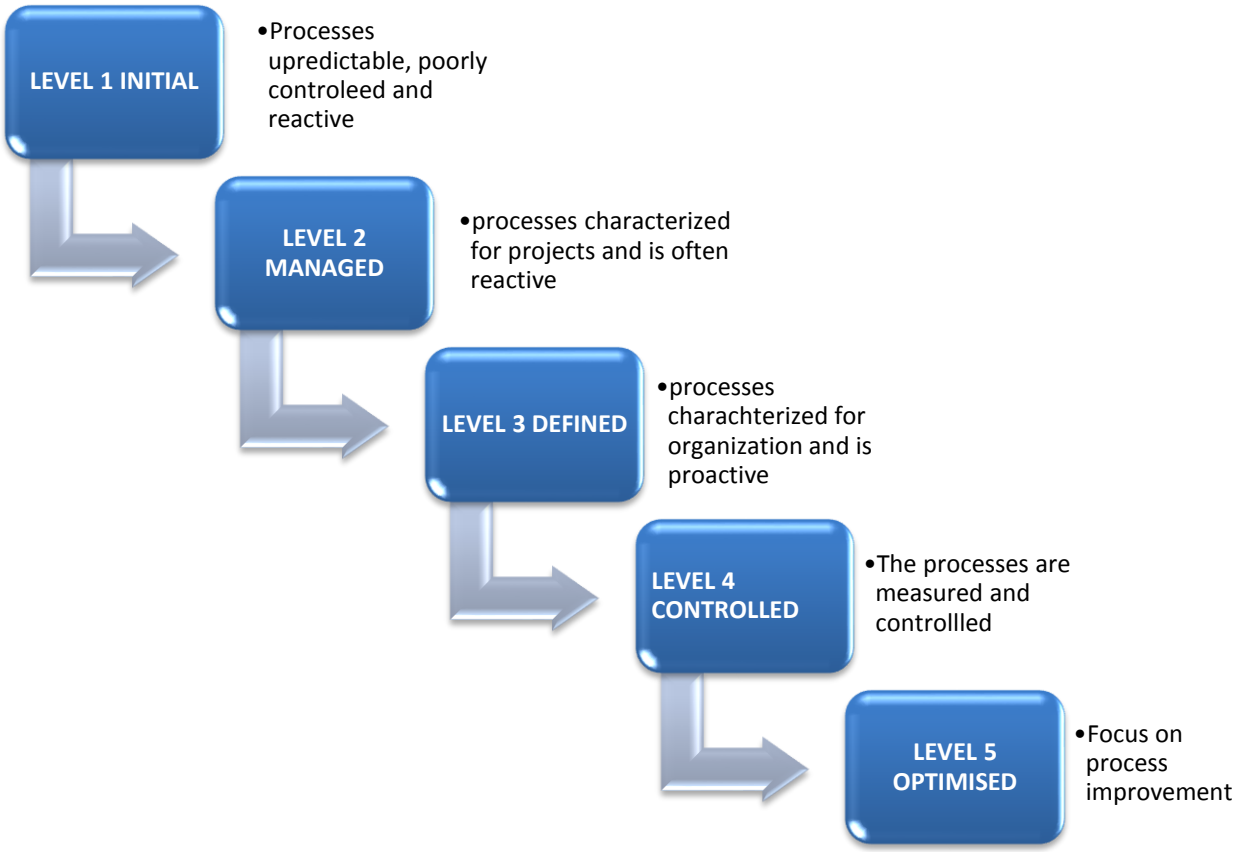
The outlines for the implementation of a data protection risk control framework are based upon law and legislation and general standards with regard to data protection. The outlines are:





6.3. Ambition – maturity level

There are 5 levels of maturity with regard to privacy:



We refer to **addendum A** for more detail about the maturity levels.

Tilburg University is currently at a level of maturity between 2 and 3. For some activities we comply with the level 3, while for others the level of maturity is level 2, as it is more based on departmental level then on organizational level. With the implementation of the AVG project in 2016/2017 we will develop towards level 3.
The ambition for Tilburg University is that we develop with regard to data protection to a level 4: controlled. In addendum B an overview is on the definition of the ambition level 4.

7. Principles for personal data processing for Tilburg University

Tilburg University shall only process personal data if it is lawful and for a dedicated purpose. The data must be accurate, relevant, and not excessive in relation to the purpose for which it is processed. Tilburg University will take appropriate organizational and technical measures against unauthorized or unlawful processing of personal data.

The general principles for processing personal data within Tilburg University are:

PRINCIPLE 1- LAWFUL AND FAIRLY

Tilburg University will only process personal data fairly and lawfully

- We have legitimate grounds for processing data, which are:
  - processing is necessary for compliance with a legal obligation to which Tilburg University is subject;
  - processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Tilburg University;
  - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
  - the data subject has given consent to the processing of his or her personal data for one or more specific purposes ;
- We do not use data in ways that have unjustified adverse effects on the individuals concerned
- We are transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data
- Handle peoples personal data only in ways they would reasonably expect;
- Make sure we do not do anything unlawful with the data.

For more detail we refer to the ***Tilburg University Data Protection Policy.***

PRINCIPLE 2 - RELATION TO PURPOSE

Tilburg University will only process personal data when there is a clear connection to purpose

- We are clear about why we are collecting personal data and what we intend to do with it
- We comply with the GDPR requirements for fair processing and provide privacy statements to individuals when processing personal data
- We ensure that when we wish to use or disclose personal data for any purpose other that is additional or different from the originaly specified purpose the new is fair and lawful.

For more detail we refer to the ***Tilburg University Data Protection Policy***

PRINCIPLE 3 - ADEQUACY

Tilburg University ensures that personal data is adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- We hold personal data about an individual that is sufficient for the purpose
- We do not hold more information than we need for this purpose.

For more detail we refer to the ***Tilburg University Data Protection Policy***

PRINCIPLE 4- RETENTION

Tilburg University will not keep personal data longer than is necessary for the purpose for which we process the data.

- We assess the lenght of time that we store personal data (legal grounds or related to purpose)
- Ensure that we delete inofmration which is:
  - no longer needed for the purpose for which we process the data
  - Exceeding the duration defined for storage.

For more detail we refer to the ***Tilburg University Data Protection Policy***

PRINCIPLE 5- RIGHTS OF INDIVIDUALS

Tilburg University ensures that we act in accordance with the rights of individuals of which we process personal data

- We will provide on request information to individuals about their data we process;
- We will delete on request personal data of individuals if legally possible
- We will adjust on request of individual their personal data when it is inaccurate;
- We will act in line with Direct Marketing legislation as defined in the Telecomwet with regard to Marketing. This means:
  - We only contact individuals that have given us their specific consent for direct marketing
  - We ensure that we do not contact individuals that have withdrawn this consent

For more detail we refer to the ***Tilburg University Data Protection Policy***

PRINCIPLE 6 - SECURITY

Tilburg University will take appropriate technical and operational measures against unauthorized and unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data

- We design and organize our security to fit the nature of the personal data we hold and the risk related to this.
- We are clear who is responsible for Information Security
- We make sure we have the right physical and technical security which is based upon robust policies and procedures and well-trained staff.
- We are ready to respond to any breaches of security swiftly and effectively.

For more detail we refer to the ***Tilburg University Information Security Policy***

PRINCIPLE 7 - INTERNATIONAL

Tilburg University will not transfer personal data to a country outside of the European Union unless we ensure an adequate level of protection of the rights and freedoms of individuals in relation to the processing of data.

- We will ensure if data is transferred outside of European Union that adequate data protection levels are implemented which are in line with European Standards.

For more detail we refer to the ***Tilburg University Data Protection Policy***

PRINCIPLE 8 - SPECIAL CATEGORIES

Tilburg University will not process special categories of Personal Data unless one of the exceptions mentioned in the GDPR is applicable

- We will ensure that when we processs special categories of peronal data it is bound by confidentiality for staffmembers who have access and have implemented the highest level of security measures (physical and technical).

7.1. Scope regarding data protection

The Scope with regard to data protection encompasses all activities in which (personal) data are processed.

Activities

All activities of Tilburg University where we process personal data are included. E.g. (not limitative): Education, Research, Human Resources, Marketing, Finance. Etc.

Storage

All storage methods in which personal data are stored are included. This means (not limitative): digital data, physical archives (internal and external) , on own servers, external servers and in the cloud.

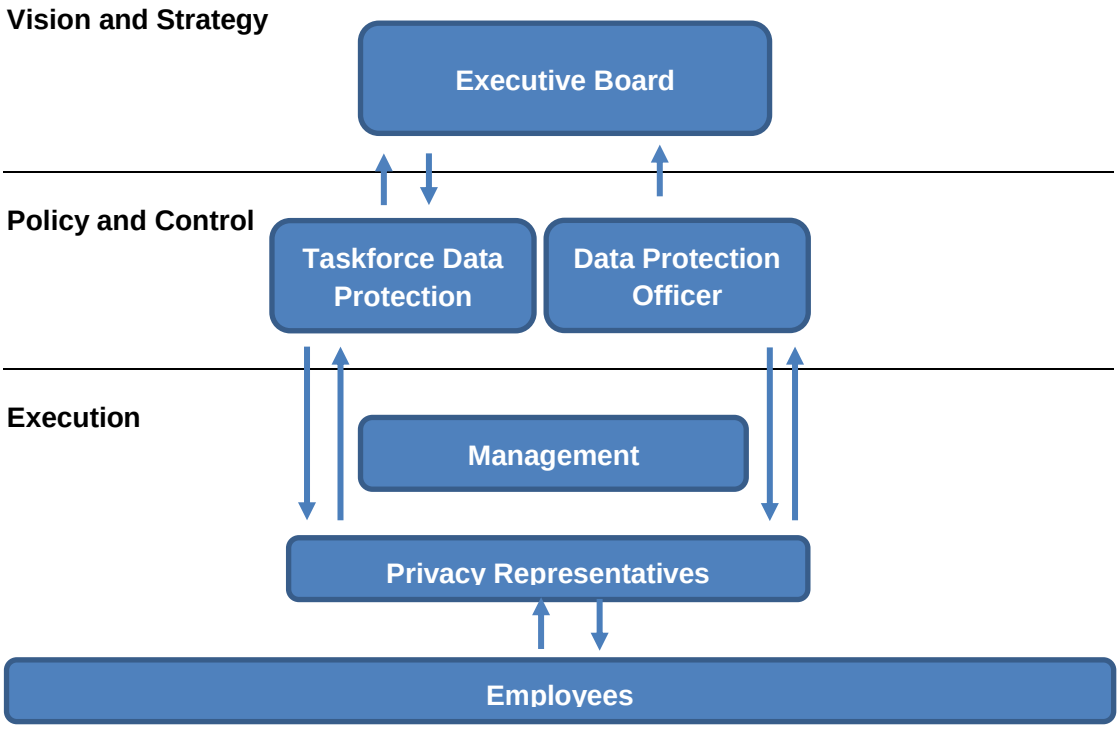
Cooperations

Tilburg University has various cooperations with other legal entities which are formalised in contractual agreements. The legal entities are accountable for compliance with the GDPR with regard to their activities. TiU will inform them about this law as there is a reputational risk involved.

8. Responsibilities with regard to Data Protection

The organization with regard to data protection must be organized. This means that people (functions) must have tasks, responsibilities and authorization with regard to Data Protection in order to effectively implement the PDCA cycle.

Data protection is the responsibility of all staff members of Tilburg University.



8.1. Responsibilities Executive Board

The Executive Board is ultimately accountable for data protection and privacy. They give instructions to define a data protection policy and allocate the necessary tasks, responsibilities with regard to data protection as well as the allocation of the means. The Chairman of the Executive Board is portfolio holder for data protection.

The Executive Board has appointed a Taskforce Data Protection and a Data Protection Officer to embed data protection in the organization, although it is the responsibility of all staffmembers to comply.

8.2. Responsibilities of Management

Management is accountable for all the processes they perform and in that role they are also accountable for data protection and privacy. They must set a good example with regard to data protection and privacy by knowing and applying the rules and defining and encouraging a culture where people are accountable for their activities and trusted. They will ensure that they comply with the GDPR and the Tilburg University Data Protection Policy and define their own internal departmental policies.

The management of divisions and faculties (directors, deans) are accountable for data protection (compliance with GDPR) for all the activities in their department / faculty. At all levels management must create an environment of individual and collective accountability in which the importance of data protection is well understood. Management achieves this part in providing sufficient resources (training, budget, staffing) to its data protection function. It is important that the staff members understand the risks and why they need to execute controls in order to mitigate these risks.

Furthermore the management is important with regard to data protection as they need to inform the Data Protection Officer in case of incidents and/or data leaks that occur in their faculty or division: They need to:

- Collect all the information with regard to the incident and report them to the Data Protection officer.
- Assist the DPO in the analysis of the incidents and take part in the follow up process by implementing corrective and preventive measures.

8.3. Responsibilities of every employee

Every employee of TiU is responsible for Data protection with regard to the activities they perform. They must understand the rules with regard to data protection and what they need to do to ensure compliance and apply them in daily operations. In cases of breaches of the rules they should immediately inform the Data Protection Officer (DPO).

8.4. Responsibilities of Task Force Data Protection

The taskforce privacy consists of representatives of the following departments:

- Legal Affairs
- Governance, Risk & Compliance
- Information Security
- Information Awareness

Depending on the subject other functions or departments may participate e.g. Human Resources or Marketing & Communication or in the field of research.

The taskforce is primarily responsible for the definition of the Tilburg University Data Protection Policy. This does not mean that the taskforce is fully responsible for the compliant processing of the personal data; they perform the following tasks.

- On request of management or privacy responsible decide on the lawful and fair (intended) processing of personal data, in order to comply with the GDPR, Internal Policies as well as other applicable law and legislation.
- Advice the Executive Board on strategic privacy matters,
- Definition of university-wide processes and procedures.
- Definition of university-wide templates (e.g. data processing agreements, DPIA etc)
- Advise on departmental policies defined by management and/or Data Protection Representatives.
- Initiate, stimulate the awareness activities.

This does not mean that the taskforce does all of this. They can appoint certain persons with certain tasks (e.g. data processing agreement template: legal affairs).

8.5. Responsibilities of Data Protection Officer (DPO)

Tilburg University has appointed a Data Protection Officer (Functionaris Gegevensbescherming) in line with the GDPR. The main law-based tasks are defined in Article 39 of the GDPR.
The data protection officer is responsible for the monitoring of the compliance of the General Data Protection Regulation (GDPR). He is not responsible for the compliance (that is the responsibility of the management). His tasks are amongst other:

- Monitor compliance with GDPR and the internal Data Protection Policy
- Monitor complete and correct inventory of the personal data Processing (Record of processing activities) in cooperation with business (methodology, register, train and facilitate)
- Monitor the execution of the Data Protection Impact Assessment and advise with regard to the DPIA.
- Answer to questions and complaints with regard to Data Protection.
- Advice with regard to policies, technology and security (privacy by design).
- Organize training, information and awareness of organization with regard to privacy.
- Contact for the Dutch Regulator: Autoriteit Persoonsgegevens.
- Collect, register and analyze data breaches and report to the regulator (Autoriteit Persoonsgegevens).

8.6. Responsibilities of Data Protection Representative (DPR)

Within the schools or divisions a Data Protection Representative (DPR) will be assigned. This person is the linking pin between the management/employees of the department and the Data Protection Officer (DPO). He/she will receive a more extensive training with regard to data protection and will be the first contact point of the department with regard to questions etc. He/she can consult the Data Protection Officer in case of complex questions / cases. He is not responsible for compliance with regard to data protection. This responsibility lies with the management.

8.7. Responsibilities of Governance, Risk & Compliance Officer

The GRC officer is member of the Taskforce and responsible for the following:

- Manage day-to-day activities with regard to Compliance
- Define and implement the compliance risk management framework in line with the general risk management framework. Drive the ongoing evolution of the Compliance Risk Framework.
- Facilitate, advice and support the faculties and department in defining the Compliance Risk Framework for their activities including training and communication support.
- Oversee Compliance Risk management activities in all faculties and divisions. Advise and support the faculties and divisions with this respect.
- Identify new or changed law and legislation and identification of the impact and necessary changes for TiU.
- Advise on all policies for TiU and advise and support the organization in in changes and processes with respect to Compliance Risk management. E.g. by participating in projects.

- Ensure adequate and timely reporting with regard to Compliance incidents and Compliance Risk management.

8.8. Responsibilities of Legal Affairs

The Legal Affairs department is a department that has an advisory and consulting role for the Executive Board, and the management (second line). A representative of Legal Affairs is participating in the Taskforce. Legal Affairs indicates the legal risks for all policies and contracts which have to be approved or signed by the Executive Board. Management can request Legal Affairs for advice (consultation). In case of implementation of (changed) laws with an impact on the whole organization the Legal Affairs department can play a coordinated role, e.g. with the implementation of the WHW and the GDPR.

8.9. Responsibilities of Information Manager

The Information manager is responsible for the management of information within a specific division or school. They need to ensure that the provision of information is effective and efficient ad in line with the requirements of the users. The information manager has an important role in the registration of personal data processing.
As they have the knowledge about the information systems and their content within their division or school they need to ensure correct and complete registration of Personal Data processing is registered in the central database (Record of Processing Activities).

8.10. Responsibilities of Chief Information Security Officer (CISO)

An important prerequisite for Data Protection is information security. The CISO is accountable for monitoring and advice with regard to information security within TiU. The CISO is participating in the Taskforce.

8.11. Responsibilities of IT Security Officer (ITSO)

An important prerequisite for Data Protection is information security. The ITSO is responsible for the technical side with regard to information security within TiU.

8.12. Responsibilities of Functioneel Beheerder (administrator)

In certain schools/ divisions there is no information manager available but there are administrators for certain tools. In this case they have an important role as they know the system and their content with regard to personal data and they are responsible for the correct and complete registration in the central database Record of Processing Activities) of all processing of personal data.

8.13. Responsibilities of Internal Audit

Internal Audit is responsible for the provision of independent, objective assurance on the overall effectiveness of the compliance with the GDPR.

In the ***Tilburg University Data Protection Policy*** the more detailed responsibilities are defined in the so-called RASCI matrix.

9. Training & Education

In order to realize the necessary knowledge and focus with regard to Data Protection it is important that we train and educate the staff members on a regular basis.

The line management is accountable for the training of the Data Protection Representatives, and this is facilitated by the Task Force Data Protection. The Data Protection Officer organizes the training and awareness. It is an annual training (extensive).
Other staff-members are trained on a regular basis in which we try to integrate the training with regard to Data Protection as much as possible in the regular training program, which is the responsibility of management. For example: researchers will be trained with this topic together with the Data Research training.

10. Allocation of means

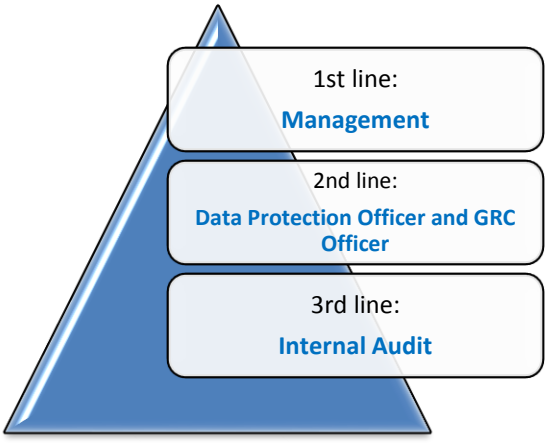
The allocation of the means with regard to data protection and security must be sufficient in order to implement the strategy with regard to data protection as defined in this document. This means in general:

- Sufficient resources:
  - For Data Protection Officer (this is based on GDPR article 38.2)
  - Data Protection Representatives
  - Supporting department like Legal Affairs and Governance, Risk & Compliance
- Sufficient financial resources in order to realize the necessary training and awareness for the organization:
  - Data Protection Officer
  - Data protection representatives
  - All other staff members:
    - Awareness-sessions
    - Information & Communication (e.g. intranet)
- Sufficient resources in order to invest in a tool to make the management of Data Protection more effective and efficient.

In the annual budget a dedicated budget will be allocated with regard to Data Protection.

11. Compliance & checks

TiU has implemented a three line of defense model to ensure compliance. For more detail we refer to the Compliance charter and framework.

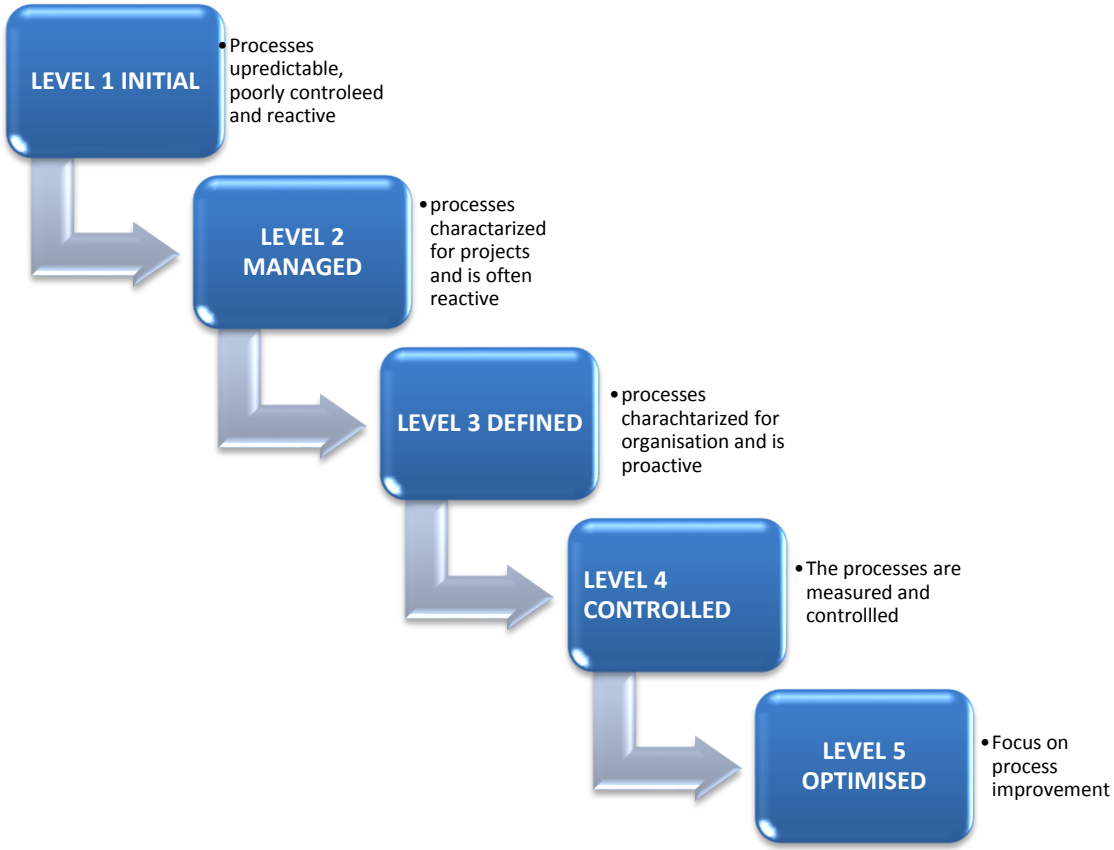


The management is responsible that for all of the activities they comply with the AVG (1st line of defense). They must implement measures (policies, procedures, checks, and training) to ensure compliance.

The compliance with the GDPR is monitored by the Data Protection Officer (Functionaris Gegevensbescherming) who acts in his role as second line of defense as well as the Governance Risk & Compliance Officer.
Breaches of the GDPR will be reported to the Executive Board by the regular incident management process and standard periodical reporting.

The third line of defense (Internal Audit) can execute compliance audits with regard to the GDPR.

ADDENDUM A – MATURITY LEVELS



Level 1: INFORMAL

On level 1 the collecting and processing of personal data is management in an informal way, which means:

- Matters are organized based upon an individual perspective, dependent on the level of knowledge and skills of the individual employee.

- There is inadequate management control to steer with policies, procedures and guidelines which means:
    - There is no formal policy for the execution of the activities (privacy policy)
    - There is limited description of the tasks, responsibilities and authorizations with regard to data protection and privacy.
    - The details on how the processing is done, is limited to the individual employees and is not shared.
- The control to comply is on an individual level:
    - There is no check on compliance
    - There is no control/assessment of the definition of processes
    - There is no PDCA-cycle for policy, execution and check.
- Improvements are not secured because of lack of standardization.

Level 2: Managed process

On level 2 the activities are performed via repeatable and standardized (controlled) processes within an individual department. There is a level of management to secure compliance within the department.

- There is a level of organization with regard to data protection within the department.
    - Departmental policies with regard to data protection
    - Involvement of stakeholders in the definition of the policies
    - There is commitment of management to steer with policies, procedures and processes within the department:
        - Existence of formal policies for the execution of the activities
        - Tasks, responsibilities and authorizations have been defined within the department
        - The knowledge about the processes is limited to the department and has a formal status.
- The level of control to comply is on a departmental level:
    - There is a departmental check on compliance
    - There is departmental control/assessment of the definition of processes
    - There is departmental PDCA-cycle for policy, execution and check.
- Improvements on organization level are not secured because of lack of

Level 3: Defined process

On level 3 the activities are performed via repeatable and standardized (controlled) processes that are defined on an organizational level. This means that on a departmental and organizational level there is control on compliance.

- There is a level of organization with regard to data protection within the organization and all departments.
    - Organizational policies with regard to data protection
    - Involvement of stakeholders in the definition of the policies and external developments are taken into account.
    - With all items with regard to data protection the organizational policies are taken as guideline.
    - Specific policies, procedures and processes are defined for standard processes and adjusted for specific projects when required. Sub processes are aligned with processed to secure control.
- There is commitment of management to steer with policies, procedures and processes within the organization which results in on organizational level:
    - Check on processing
    - Control / assessment of the definition of the services provided
    - Management cycle for policies, execution and check.
- Standard processes are used to ensure consistency of processing within the organization, which ensures that organizational improvements are not lost and we can pro-actively manage processes.

Level 4: Controlled process

On level 4 the activities are performed while the qualitative and quantitative performance is measured on a regular basis based upon detailed information.

- There is relation between external requirements, strategy of the organization, other policies (e.g. security) and the processing (with audit trail). The activities are controlled on a departmental as well as organizational level.
- The control is in addition to the requirements in level 3 based upon predictions that can be made on statistical and quantitative analyses of detailed process details. This implies:
    - Quantitative goals have been defined for quality, performance and projects
    - The quantitative goals have been defined taking into account the customer needs, the end users, organization and processors.
    - The quality and process performance is measured in statistical terms
    - The performance results are collected and analyzed
    - The quality and performance is the basis of the management of processes and projects.

Level 5: Optimized process

On level 5 the activities are performed while the qualitative and quantitative performance is measured on a regular basis based upon detailed information in order to optimize the performance. In addition to level 4 this implies:

- There is excellence control, benchmarking, innovation and process optimization.
- The performance is measured via an (automized) dashboard, based upon continuous measurement
- The management is managing the total performance o the organization, by analyzing the performance of multiple projects/processes:
    - Analyzing of performance data to identify gaps or incidents
    - Gaps and incidents are used to identify improvements to optimize performance.
    - The organization can be dynamically adjusted based upon practical experiences and prognoses.
    - The learning ability (and adjustability) of the organization is optimized:
        - The effectivity of improvements is measured.

On the various arears the assessment criteria are designed based upon the maturity model which is defined by the Centrum voor Informatiebeveiliging en privacy bescherming.

	Privacy criterium	Ambition – level 4
processor	The organization has defined privacy policies and procedures which define the method of processing of personal data and the legal requirements	• TiU monitors pro-actively the developments in law and legislation and codes of conducts regarding data protection in order to assess impact timely and adjust the policies and procedures accordingly. • The quality (usability and up to date) of the policies and procedures is measurable and formalized at every level.
Organization	The definition of tasks, responsibilities and authorizations, means and reporting lines regarding data protection have been defined and formalized	• External developments, including relevant law and legislation and codes of conduct applicable for all universities, are actively monitored by the organization, in order to assess the impact on the organization and implement immediately the necessary changes.
Riskmanagement, Privacy by design	The responsible processor ensures that the data protection risks are assessed and that adequate measures are implemented	• Standard risk management methodology implemented which included data protection risks. Risk management approach is defined and formalized and based upon the plan-do-check-act principle. • Knowledge about the risks (on need to know principle) is up to date and complete for the organization.

		• There is a complete and up to date picture of data protection risks related to the operations. • The risks are assessed and impact is defined, and proactively mitigated (if necessary). • With new activities / projects a DPIA is executed to assess data protection risk and define mitigating measures.
Connection to purpose	The responsible processor has a registration of all data collections in which specifically is defined (up to date) all the aspects that are required by the GDPR.	• For all data collections containing personal data a standardized uniform registration is available for the whole university (in 1-registration system, via standardized methodology). • The monitoring of compliance is done for the whole organization. • The assessment of the justification grounds is done based upon a standardized (branch specific) methodology. Developments with regard to this justification grounds are monitored and pro-actively taken into account.
Processing register	The responsible controller and processor have registered all data processing in a register. This register provided an up-to-date, consistent picture of all data collections, processes and technical systems that are involved.	• The organization has a complete and up-to-date overview of all data processing activities which are defined and formalized. • The connection between processes, systems and data is visible and available for the whole organization and gives overview at all levels. • The information about the personal data and processing is taken into account in decision-taking with regard to changes. • The processing register is integral part of the processes to ensure efficiency and effectivity with regard to protection of privacy. • The process in order to keep this register up to date is part of the organization wide data and architecture processes.
Quality management	The accountable controller has embedded quality management to ensure the correctness of personal data. The processes are defined in a way that data can be adjusted, deleted or transferred. If this is on request of an individual he is informed.	• The quality of personal data is controlled on an organization wide level and formally defined, including the policies and procedures with regard to the right of adjustments, delete and transferred). • This control is implemented on all levels of the organization. • The information to the individual that requests it is informed via standardized procedure. • Quality management is an integrated part of the management system in order to effectively and efficiently ensure compliance with regard to data protection. • Quality management system is in line with branch standards.
Security and protection	The accountable controller and processor ensure technical and operational measures in order to secure the data protection at an adequate level	• Information management is based upon an ISMS (Information Security Management system) an integral part of the plan and control cycle of the organization. • The effectivity of the information security is measured via KPI's in order to steer on department/activity level. • Security incidents are (in case possible) prevented by monitoring (potential) data breaches.

		• External developments (branch related) are monitored in order to make necessary changes. •
Information	The accountable controller ensures that the individual is informed in a timely manner about the (specific) data collection. The individual can give his specific consent with regard to the data collection.	• The providing of information is done on via standardized process which is organization wide. • There is an organization wide policy that defines the standard for information and requirements. • The information is based upon the standards that are set in de university-branch • The customer satisfaction is assessed and improvement measures are implemented if required.
Storage	The organization has implemented a policy with regard to maximum storage duration and secures that this is not exceeded	• There is an organization wide policy with regard to storage duration of specific data that is in line with branch standards • Developments in university branch is monitored • The destruction of data is done via branch standard procedures.
Transfer of data	The transfer of data is performed in line with the standards defined in the GDPR	• There is a data transfer policy for the whole organization which is in line with branch specific standards • The task, responsibilities and authorisations have been defined and formalized • The procedure for data transfer is standardized.
Internal control	There is an audit / check performed on the legitimacy	• A DPO has been appointed • The monitoring of the legitimacy of data processing is an integral part of the management and risk control proceses • The organization has standardized methodology for monitoring which is line with branch standard • The effectivity of the control is part of the strategy and policy.
Access to data by individuals	The accountable controller provides information to the individuals in a timely and suitable manner to ensure that individuals can execute all of their rights unless an exception is applicable.	• There is an organization wide, formalized policy and procedure regarding the execution of the right of the individuals in line witht branch standard. • The exception grounds are formalized via a predefined procedure • Reporting about requested and provided rights. • Assessment of the compliance with the rights is integrated in the (risk) management & control framework.
Data breaches	The accountable controller reports a data breach within the timeframe required to the AP. He makes registration, informs the involved unless exception applicable.	• The procedure regarding reporting of data braches is formalized and integral part of the ISMS system. • Data breaches are prevented as much as possible by monitoring (potential) data breaches

		• Knowledge around data breaches is monitored and shared within and outside Tilburg University. • Prevention of data braches is monitored via KPI's and used for improvement. • The prevention of data breaches is part of the design process (privacy by design)